

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN  
PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

SIEMENS AKTIENGESELLSCHAFT  
Postfach 22 16 34  
80506 München  
ALLEMAGNE

ZT GG VM Mch P/Ri

Eing. 22 Jan. 2001

GR  
Frist

30.01.01

## PCT

MITTEILUNG ÜBER DIE ÜBERSENDUNG  
DES INTERNATIONALEN VORLÄUFIGEN  
PRÜFUNGSBERICHTS  
(Regel 71.1 PCT)

Absendedatum  
(Tag/Monat/Jahr)

19.01.2001

Aktenzeichen des Anmelders oder Anwalts  
98P2821P

### WICHTIGE MITTEILUNG

Internationales Aktenzeichen  
PCT/DE99/02844

Internationales Anmeldedatum (Tag/Monat/Jahr)  
08/09/1999

Prioritätsdatum (Tag/Monat/Jahr)  
30/09/1998

Anmelder

SIEMENS AKTIENGESELLSCHAFT et al.

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Prüfungsbericht, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.
2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.
3. Auf Wunsch eines ausgewählten Amtes wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.
4. **ERINNERUNG**

Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Prüfungsbericht enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde



Europäisches Patentamt  
D-80298 München  
Tel. +49 89 2399 - 0 Tx: 523656 epmu d  
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter

Koski, P

Tel. +49 89 2399-2709



# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT

### INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT



(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts 98P2821P	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE99/02844	Internationales Anmeldedatum (Tag/Monat/Jahr) 08/09/1999	Prioritätsdatum (Tag/Monat/Jahr) 30/09/1998
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G06F1/00		
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.  
  
☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).  
  
Diese Anlagen umfassen insgesamt 2 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☒ Bestimmte Mängel der internationalen Anmeldung
- VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags  07/03/2000	Datum der Fertigstellung dieses Berichts  19.01.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:   Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter  Harms, C  Tel. Nr. +49 89 2399 7476  

**I. Grundlage des Berichts**

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten.*):

**Beschreibung, Seiten:**

1-17                      ursprüngliche Fassung

**Patentansprüche, Nr.:**

2-8,10-12              ursprüngliche Fassung

1,9                      eingegangen am                      01/12/2000    mit Schreiben vom    30/11/2000

**Zeichnungen, Blätter:**

1-3                      ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

# INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE99/02844

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung,      Seiten:
- ☐ Ansprüche,      Nr.:
- ☐ Zeichnungen,      Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

*(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).*

6. Etwaige zusätzliche Bemerkungen:

## V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	2-8, 10-12
	Nein: Ansprüche	1, 9
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	
	Nein: Ansprüche	1-12
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-12
	Nein: Ansprüche	

2. Unterlagen und Erklärungen  
**siehe Beiblatt**

## VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:  
**siehe Beiblatt**

## VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:  
**siehe Beiblatt**

**ZU PUNKT V**

Es wird auf folgende Dokumente verwiesen:

D1: HP-UX 11.00 Manual

([http://www.devresource.hp.com/STK/man/11.00/passwd\\_1.html](http://www.devresource.hp.com/STK/man/11.00/passwd_1.html))

D2: Deborah Russell, G.T. Gangemi Sr: Computer Security Basics, July 1992, O'Reilly & Associates.

Beide Dokumente sind im internationalen Recherchenbericht nicht angegeben. Eine Kopie des Dokuments D1 wurde dem Anmelder mit der Niederschrift über das Telefonat vom 23.11.2000 übermittelt. Eine Kopie des Dokuments D2 liegt diesem Prüfungsbericht bei.

- 1 Der Gegenstand des Hauptanspruchs 1 ist nicht neu, weil D1 folgenden Stand der Technik offenbart; Art. 33(2) PCT:

Die Merkmale a) -d) beschreiben die typischen Ablauf einer Client-Server Sitzung: Der Client wird in den Ansprüchen als "erster Rechner" bezeichnet, der Server als "zweiter Rechner". Die Dienstanforderung des Clients ist zusätzlich mit einem Paßwort gesichert. Für den Fall, daß das Paßwort gültig ist, wird der Dienst ausgeführt, andernfalls nicht. Dies ist gängige Praxis z.B. bei den Diensten FTP (file transfer protocol) und telnet. Beide Dienste sind standardmäßig in Unix implementiert, gehören aber nicht zum eigentlichen Betriebssystemkern (kernel). Sie werden als Dienstprogramme bezeichnet, weil sie einen Dienst (internet service) realisieren.

Die Merkmale e) und f) sind beide aus dem Dokument D1 ersichtlich. Der Ablauf eines Paßwortes kann vom Superuser mit der Option -x festgelegt werden. Bei der ersten Inanspruchnahme des Dienstes (wie z.B. FTP oder telnet) nach Ablauf des Paßwortes wird der Benutzer aufgefordert, daß Paßwort zu aktualisieren. Dazu wird vom Betriebssystem passwd [name] mit der user ID als Parameter aufgerufen. Alternativ kann das Paßwort auch vom Server geändert werden. Vor- und Nachteile von Benutzer- und Systemgenerierten Paßwörtern sind allgemein bekannt und werden z.B. in D2 diskutiert.

- 2 Der Hauptanspruch 9 definiert die dem Verfahrensanspruch 1 entsprechende

Vorrichtung und ist daher ebenfalls nicht neu; Art. 33(2) PCT.

- 3 Die abhängigen Ansprüche 2-8 und 10-11 definieren geringfügige Änderungen zu ihren jeweiligen Hauptansprüchen und sind als nicht erfinderisch anzusehen (Art. 33(3) PCT). Die im Recherchenbericht zitierten Dokumente offenbaren zahlreiche Vorrichtungen und Methoden zur sicheren Übertragung von Paßwörtern zwischen Client und Server (Authentifizierung, Verschlüsselung zur Integritätssicherung, Zugriffskontrolle).

#### ZU PUNKT VII

- 1 Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT werden in der Beschreibung weder der in dem Dokument D1 offenbarte einschlägige Stand der Technik noch dieses Dokument angegeben.
- 2 Die Beschreibung von Seite 3 Zeile 13 bis Seite 4 Zeile 26 hätte in Einklang mit den neu eingereichten Ansprüchen 1 und 9 gebracht werden sollen; Regel 5.1 a) iii) PCT.

#### ZU PUNKT VIII

- 1 Im Hauptanspruch 1 Zeile 18 und im Hauptanspruch 9 Zeile 22 sollte "ungültig" in Zeile 18 durch "abgelaufen" ersetzt werden. Die Aktualisierung eines ungültigen Paßworts (d.h. eines Paßwortes, das nie gültig war) würde keinen Sinn ergeben. Diese Änderung wäre zulässig gewesen, weil sie sich auf die ursprüngliche Beschreibung auf Seite 1 Zeilen 22-29 stützt.
- 2 Die Merkmale der Ansprüche 1-12 sind nicht mit in Klammern gesetzten Bezugszeichen versehen worden (Regel 6.2 b) PCT).

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN  
PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

SIEMENS AKTIENGESELLSCHAFT  
Postfach 22 16 34  
80506 München  
ALLEMAGNE

## PCT

MITTEILUNG ÜBER FORMLOSE  
ERÖRTERUNGEN MIT DEM ANMELDER

(Regel 66.6 PCT)

Absendedatum  
(Tag/Monat/Jahr) 19.01.2001

Aktenzeichen des Anmelders oder Anwalts  
98P2821P

**ÜBERSENDUNG ZUR INFORMATION**

Internationales Aktenzeichen  
PCT/DE99/02844

Internationales Anmeldedatum (Tag/Monat/Jahr)  
08/09/1999

Anmelder

SIEMENS AKTIENGESELLSCHAFT et al.

Am 10/01/2001 fand eine formlose Erörterung zwischen der mit der internationalen vorläufigen Prüfung beauftragten Behörde und dem Anmelder / dem Anwalt statt.

Eine Kopie der Niederschrift über diese Erörterung (Formblatt PCT/IPEA/428) wird Ihnen beiliegend zur Unterrichtung übermittelt.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde



Europäisches Patentamt  
D-80298 München  
Tel. +49 89 2399 - 0 Tx: 523656 epmu d  
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter

Koski, P

Telefon +49 89 2399-2709



**Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens**  
**Patent Cooperation Treaty**  
**Traité de coopération en matière de brevets**

**PCT**

Anmeldenummer:

PCT/DE99/02844

**Niederschrift über eine telefonische formlose Erörterung mit dem Anmelder**

Eine Kopie dieser Niederschrift wird dem Anmelder zur Unterrichtung übermittelt

**Teilnehmer**

Anmelder: Siemens Aktiengesellschaft

Anwalt: Dr. Wolfgang Schwarz

Prüfer: Harms, C

**Zusammenfassung der Erörterung**

Der Anmelder hat den zuständigen Prüfer für den Fall eines negativen vorläufigen Prüfungsbericht um informelle Rücksprache gebeten.

10/01/2001

.....  
Datum (Tag / Monat / Jahr)



Harms, C

.....  
Bevollmächtigter Bediensteter der mit der  
internationalen vorläufigen Prüfung  
beauftragten Behörde



01-12-2000

1998P02821WO

PCT/DE99/02844

18

**Patentansprüche**

1. Verfahren zur Aktualisierung eines Paßwortes zwischen einem ersten Rechner und einem zweiten Rechner,

- 5 a) bei dem der zweite Rechner im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht eines Dienstprogramms empfängt, wobei die Dienstanforderungsnachricht das Paßwort
- 10 aufweist,
- b) bei dem mit der Dienstanforderungsnachricht von dem ersten Rechner die Erbringung eines Dienstes angefordert wird,
- c) bei dem der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den
- 15 ersten Rechner gültig ist,
- d) bei dem für den Fall, daß das Paßwort gültig ist, der Dienst erbracht wird,
- e) bei dem für den Fall, daß das Paßwort ungültig ist, von dem zweiten Rechner eine Aktualisierungsnachricht an den
- 20 ersten Rechner gesendet wird, mit der eine Aktualisierung des Paßworts gefordert wird, und
- f) bei dem von dem ersten Rechner oder dem zweiten Rechner ein aktualisiertes Paßwort gebildet wird, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort
- 25 verwendet wird.

2. Verfahren nach Anspruch 1,

bei dem die Bildung des aktualisierten Paßwortes auf folgende Weise erfolgt:

- 30 a) der erste Rechner sendet eine Paßwortnachricht zu dem zweiten Rechner, in der das aktualisierte Paßwort enthalten ist in einer Weise, daß das aktualisierte Paßwort nur unter Verwendung des Paßwortes ermittelt werden kann,
- b) der zweite Rechner ermittelt unter Verwendung des Paßwortes das aktualisierte Paßwort aus der Paßwortnachricht,
- 35 c) der zweite Rechner speichert das aktualisierte Paßwort.

bei dem der Schlüssel durch mehrfache Aneinanderreihung des Paßwortes gebildet wird.

5 9. Anordnung mit mindestens einem ersten Rechner und mindestens einem zweiten Rechner zur Aktualisierung eines Paßwortes zwischen den Rechnern,

wobei der erste Rechner und der zweite Rechner jeweils einen Prozessor aufweisen, die derart eingerichtet sind, daß folgende Schritte durchführbar sind:

- 10 a) der zweite Rechner empfängt im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht eines Dienstprogramms, wobei die Dienstanforderungsnachricht das Paßwort aufweist,
- 15 b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,
- c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,
- 20 d) für den Fall, daß das Paßwort gültig ist, wird der Dienst erbracht,
- e) für den Fall, daß das Paßwort ungültig ist, wird von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet, mit der eine Aktualisierung des Paß-
- 25 worts gefordert wird, und
- f) von dem ersten Rechner oder dem zweiten Rechner wird ein aktualisiertes Paßwort gebildet, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

30

10. Anordnung nach Anspruch 9, bei der die Prozessoren derart eingerichtet sind, daß die Bildung des aktualisierten Paßwortes auf folgende Weise erfolgt:

- 35 a) der erste Rechner sendet eine Paßwortnachricht zu dem zweiten Rechner, in der das aktualisierte Paßwort enthal-

Patent claims

1. A method for updating a password between a first computer and a second computer,

5 a) in which the second computer receives a service request message, for a service program, transmitted by the first computer over a communication link existing between the first computer and the second computer, with the service request message containing the  
10 password,

b) in which the service request message from the first computer is used to request provision of a service,

c) in which the second computer checks whether the  
15 password contained in the service request message is valid for the first computer,

d) in which, if the password is valid, the service is provided,

e) in which, if the password is invalid, the  
20 second computer transmits to the first computer an update message which is used to request that the password be updated, and

f) in which the first computer or the second computer forms an updated password which is  
25 subsequently used as the password within the context of the communication link.

2. The method as claimed in claim 1,

in which the updated password is formed in the following manner:

30 a) the first computer transmits to the second computer a password message, containing the updated password, such that the updated password can be ascertained only by using the password,

b) the second computer uses the password to  
35 ascertain the updated password from the password message,

AMENDED SHEET

*do not enter*

December 2000  
1998P02821WO  
PCT/DE99/02844

DE 009902844

- 18a -

c) the second computer stores the updated  
password.

AMENDED SHEET

- 20 -

in which the key is formed by stringing together the password a number of times.

9. An arrangement having at least one first computer and at least one second computer for updating  
5 a password between the computers,

the first computer and the second computer each having a processor which is set up such that the following steps can be carried out:

a) the second computer receives a service request  
10 message, for a service program, transmitted by the first computer over a communication link existing between the first computer and the second computer, with the service request message containing the password,

15 b) the service request message from the first computer is used to request provision of a service,

c) the second computer checks whether the password contained in the service request message is valid for the first computer,

20 d) if the password is valid, the service is provided,

e) if the password is invalid, the second computer transmits to the first computer an update message which is used to request that the password be updated, and

25 f) the first computer or the second computer forms an updated password which is subsequently used as the password within the context of the communication link.

10. The arrangement as claimed in claim 9,  
in which the processors are set up such that the  
30 updated password is formed in the following manner:

a) the first computer transmits to the second computer a password message, containing the updated

AMENDED SHEET

*Do not enter*

## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<b>(51) International patent classification<sup>7</sup>:</b>  G06F 1/00	<b>A1</b>	<b>(11) International publication number:</b> WO 00/19297  <b>(43) International publication date:</b> 6 April 2000 (06.04.00)
<b>(21) International application number:</b> PCT/DE99/02844 <b>(22) International filing date:</b> 8 September 1999 (08.09.99)  <b>(30) Data relating to the priority:</b> 198 45 055.9 30 September 1998 (30.09.98) DE  <b>(71) Applicant (for all designated States except US):</b> SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-80333 Munich (DE).  <b>(72) Inventors; and</b> <b>(75) Inventors/Applicants (US only):</b> FRIES, Steffen [DE/DE]; Wagenbauerstrasse 5, D-81677 Munich (DE). EUCHNER, Martin [DE/DE]; Lorenzstrasse 2, D-81737 Munich (DE).  <b>(74) Joint Representative:</b> SIEMENS AKTIENGE- SELLSCHAFT; Postfach 22 16 34, D-80506 Munich (DE).		<b>(81) Designated states:</b> US, European Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  <b>Published</b> With the International Search Report. Before expiry of the period provided for amending the claims, will be republished if such amendments are received.

As printed

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

## PCT

MITTEILUNG ÜBER DIE ÜBERMITTLUNG DES  
INTERNATIONALEN RECHERCHENBERICHTS  
ODER DER ERKLÄRUNG

(Regel 44.1 PCT)

An

SIEMENS AKTIENGESELLSCHAFT  
Postfach 22 16 34  
80506 München  
GERMANY

ZT GG V. Moh P/R

Eing. 28. Feb. 2000

GR  
Frist

Absenddatum  
(Tag/Monat/Jahr)

24/02/2000

Aktenzeichen des Anmelders oder Anwalts

98P2821P

WEITERES VORGEHEN

siehe Punkte 1 und 4 unten

Internationales Aktenzeichen

PCT/DE 99/02844

Internationales Anmeldedatum

(Tag/Monat/Jahr)

08/09/1999

Anmelder

SIEMENS AKTIENGESELLSCHAFT et al.

1. ☒ Dem Anmelder wird mitgeteilt, daß der Internationale Recherchenbericht erstellt wurde und ihm hiermit übermittelt wird.

**Einreichung von Änderungen und einer Erklärung nach Artikel 19:**

Der Anmelder kann auf eigenen Wunsch die Ansprüche der Internationalen Anmeldung ändern (siehe Regel 46):

**Bis wann sind Änderungen einzureichen?**

Die Frist zur Einreichung solcher Änderungen beträgt üblicherweise zwei Monate ab der Übermittlung des Internationalen Recherchenberichts; weitere Einzelheiten sind den Anmerkungen auf dem Beiblatt zu entnehmen.

**Wo sind Änderungen einzureichen?**

Unmittelbar beim Internationalen Büro der WIPO, 34, CHEMIN des Colombettes, CH-1211 Genf 20,  
Telefaxnr.: (41-22) 740.14.35

Nähere Hinweise sind den Anmerkungen auf dem Beiblatt zu entnehmen.

2. ☐ Dem Anmelder wird mitgeteilt, daß kein Internationaler Recherchenbericht erstellt wird und daß ihm hiermit die Erklärung nach Artikel 17(2)a) übermittelt wird.

3. ☐ Hinsichtlich des Widerspruchs gegen die Entrichtung einer zusätzlichen Gebühr (zusätzlicher Gebühren) nach Regel 40.2 wird dem Anmelder mitgeteilt, daß

☐ der Widerspruch und die Entscheidung hierüber zusammen mit seinem Antrag auf Übermittlung des Wortlauts sowohl des Widerspruchs als auch der Entscheidung hierüber an die Bestimmungsämter dem Internationalen Büro übermittelt worden sind.

☐ noch keine Entscheidung über den Widerspruch vorliegt; der Anmelder wird benachrichtigt, sobald eine Entscheidung getroffen wurde.

4. **Weiteres Vorgehen:** Der Anmelder wird auf folgendes aufmerksam gemacht:

Kurz nach Ablauf von 18 Monaten seit dem Prioritätsdatum wird die internationale Anmeldung vom Internationalen Büro veröffentlicht. Will der Anmelder die Veröffentlichung verhindern oder auf einen späteren Zeitpunkt verschieben, so muß gemäß Regel 90<sup>bis</sup> bzw. 90<sup>ter</sup> vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung eine Erklärung über die Zurücknahme der internationalen Anmeldung oder des Prioritätsanspruchs beim Internationalen Büro eingehen.

Innerhalb von 19 Monaten seit dem Prioritätsdatum ist ein Antrag auf internationale vorläufige Prüfung einzureichen, wenn der Anmelder den Eintritt in die nationale Phase bis zu 30 Monaten seit dem Prioritätsdatum (in manchen Ämtern sogar noch länger) verschieben möchte.

Innerhalb von 20 Monaten seit dem Prioritätsdatum muß der Anmelder die für den Eintritt in die nationale Phase vorgeschriebenen Handlungen vor allen Bestimmungsämtern vornehmen, die nicht innerhalb von 19 Monaten seit dem Prioritätsdatum in der Anmeldung oder einer nachträglichen Auswahlerklärung ausgewählt wurden oder nicht ausgewählt werden konnten, da für sie Kapitel II des Vertrages nicht verbindlich ist.

Name und Postanschrift der Internationalen Recherchenbehörde



Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL-2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+31-70) 340-3016

Bevollmächtigter Bediensteter

Marja Brouwers

Diese Anmerkungen sollen grundlegende Hinweise zur Einreichung von Änderungen gemäß Artikel 19 geben. Diesen Anmerkungen liegen die Erfordernisse des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), der Ausführungsordnung und der Verwaltungsrichtlinien zu diesem Vertrag zugrunde. Bei Abweichungen zwischen diesen Anmerkungen und obengenannten Texten sind letztere maßgebend. Nähere Einzelheiten sind dem PCT-Leitfaden für Anmelder, einer Veröffentlichung der WIPO, zu entnehmen.

Die in diesen Anmerkungen verwendeten Begriffe "Artikel", "Regel" und "Abschnitt" beziehen sich jeweils auf die Bestimmungen des PCT-Vertrags, der PCT-Ausführungsordnung bzw. der PCT-Verwaltungsrichtlinien.

## **HINWEISE ZU ÄNDERUNGEN GEMÄSS ARTIKEL 19**

Nach Erhalt des internationalen Recherchenberichts hat der Anmelder die Möglichkeit, einmal die Ansprüche der internationalen Anmeldung zu ändern. Es ist jedoch zu betonen, daß, da alle Teile der internationalen Anmeldung (Ansprüche, Beschreibung und Zeichnungen) während des internationalen vorläufigen Prüfungsverfahrens geändert werden können, normalerweise keine Notwendigkeit besteht, Änderungen der Ansprüche nach Artikel 19 einzureichen, außer wenn der Anmelder z. B. zum Zwecke eines vorläufigen Schutzes die Veröffentlichung dieser Ansprüche wünscht oder ein anderer Grund für eine Änderung der Ansprüche vor ihrer internationalen Veröffentlichung vorliegt. Weiterhin ist zu beachten, daß ein vorläufiger Schutz nur in einigen Staaten erhältlich ist.

### **Welche Teile der internationalen Anmeldung können geändert werden?**

Im Rahmen von Artikel 19 können nur die Ansprüche geändert werden.

In der internationalen Phase können die Ansprüche auch nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert (oder nochmals geändert) werden. Die Beschreibung und die Zeichnungen können nur nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert werden.

Beim Eintritt in die nationale Phase können alle Teile der internationalen Anmeldung nach Artikel 28 oder gegebenenfalls Artikel 41 geändert werden.

### **Bis wann sind Änderungen einzureichen?**

Innerhalb von zwei Monaten ab der Übermittlung des internationalen Recherchenberichts oder innerhalb von sechzehn Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft. Die Änderungen gelten jedoch als rechtzeitig eingereicht, wenn sie dem Internationalen Büro nach Ablauf der maßgebenden Frist, aber noch vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung (Regel 46.1) zugehen.

### **Wo sind die Änderungen nicht einzureichen?**

Die Änderungen können nur beim Internationalen Büro, nicht aber beim Anmeldeamt oder der Internationalen Recherchenbehörde eingereicht werden (Regel 46.2).

Falls ein Antrag auf internationale vorläufige Prüfung eingereicht wurde/wird, siehe unten.

### **In welcher Form können Änderungen erfolgen?**

Eine Änderung kann erfolgen durch Streichung eines oder mehrerer ganzer Ansprüche, durch Hinzufügung eines oder mehrerer neuer Ansprüche oder durch Änderung des Wortlauts eines oder mehrerer Ansprüche in der eingereichten Fassung.

Für jedes Anspruchsblatt, das sich aufgrund einer oder mehrerer Änderungen von dem ursprünglich eingereichten Blatt unterscheidet, ist ein Ersatzblatt einzureichen.

Alle Ansprüche, die auf einem Ersatzblatt erscheinen, sind mit arabischen Ziffern zu numerieren. Wird ein Anspruch gestrichen, so brauchen die anderen Ansprüche nicht neu numeriert zu werden. Im Fall einer Neunummerierung sind die Ansprüche fortlaufend zu numerieren (Verwaltungsrichtlinien, Abschnitt 205 b)).

Die Änderungen sind in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

### **Welche Unterlagen sind den Änderungen beizufügen?**

**Begleitschreiben (Abschnitt 205 b)):**

Die Änderungen sind mit einem Begleitschreiben einzureichen.

Das Begleitschreiben wird nicht zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht. Es ist nicht zu verwechseln mit der "Erklärung nach Artikel 19(1)" (siehe unten, "Erklärung nach Artikel 19 (1)").

Das Begleitschreiben ist nach Wahl des Anmelders in englischer oder französischer Sprache abzufassen. Bei englischsprachigen internationalen Anmeldungen ist das Begleitschreiben aber ebenfalls in englischer, bei französischsprachigen internationalen Anmeldungen in französischer Sprache abzufassen.



## ANMERKUNGEN ZU FORMBLATT PCT/ISA/220 (Übersetzung)

Im Begleitschreiben sind die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen anzugeben. So ist insbesondere zu jedem Anspruch in der internationalen Anmeldung anzugeben (gleichlautende Angaben zu verschiedenen Ansprüchen können zusammengefaßt werden), ob

- i) der Anspruch unverändert ist;
- ii) der Anspruch gestrichen worden ist;
- iii) der Anspruch neu ist;
- iv) der Anspruch einen oder mehrere Ansprüche in der eingereichten Fassung ersetzt;
- v) der Anspruch auf die Teilung eines Anspruchs in der eingereichten Fassung zurückzuführen ist.

Im folgenden sind Beispiele angegeben, wie Änderungen im Begleitschreiben zu erläutern sind:

1. [Wenn anstelle von ursprünglich 48 Ansprüchen nach der Änderung einiger Ansprüche 51 Ansprüche existieren]:  
"Die Ansprüche 1 bis 29, 31, 32, 34, 35, 37 bis 48 werden durch geänderte Ansprüche gleicher Numerierung ersetzt; Ansprüche 30, 33 und 36 unverändert; neue Ansprüche 49 bis 51 hinzugefügt."
2. [Wenn anstelle von ursprünglich 15 Ansprüchen nach der Änderung aller Ansprüche 11 Ansprüche existieren]:  
"Geänderte Ansprüche 1 bis 11 treten an die Stelle der Ansprüche 1 bis 15."
3. [Wenn ursprünglich 14 Ansprüche existierten und die Änderungen darin bestehen, daß einige Ansprüche gestrichen werden und neue Ansprüche hinzugefügt werden]:  
"Ansprüche 1 bis 6 und 14 unverändert; Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt. "Oder" Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt; alle übrigen Ansprüche unverändert."
4. [Wenn verschiedene Arten von Änderungen durchgeführt werden]:  
"Ansprüche 1-10 unverändert; Ansprüche 11 bis 13, 18 und 19 gestrichen; Ansprüche 14, 15 und 16 durch geänderten Anspruch 14 ersetzt; Anspruch 17 in geänderte Ansprüche 15, 16 und 17 unterteilt; neue Ansprüche 20 und 21 hinzugefügt."

### "Erklärung nach Artikel 19(1)" (Regel 46.4)

Den Änderungen kann eine Erklärung beigelegt werden, mit der die Änderungen erläutert und ihre Auswirkungen auf die Beschreibung und die Zeichnungen dargelegt werden (die nicht nach Artikel 19 (1) geändert werden können).

Die Erklärung wird zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht.

Sie ist in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Sie muß kurz gehalten sein und darf, wenn in englischer Sprache abgefaßt oder ins Englische übersetzt, nicht mehr als 500 Wörter umfassen.

Die Erklärung ist nicht zu verwechseln mit dem Begleitschreiben, das auf die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen hinweist, und ersetzt letzteres nicht. Sie ist auf einem gesonderten Blatt einzureichen und in der Überschrift als solche zu kennzeichnen, vorzugsweise mit den Worten "Erklärung nach Artikel 19 (1)".

Die Erklärung darf keine herabsetzenden Äußerungen über den internationalen Recherchenbericht oder die Bedeutung von in dem Bericht angeführten Veröffentlichungen enthalten. Sie darf auf im internationalen Recherchenbericht angeführte Veröffentlichungen, die sich auf einen bestimmten Anspruch beziehen, nur im Zusammenhang mit einer Änderung dieses Anspruchs Bezug nehmen.

### Auswirkungen eines bereits gestellten Antrags auf internationale vorläufige Prüfung

Ist zum Zeitpunkt der Einreichung von Änderungen nach Artikel 19 bereits ein Antrag auf internationale vorläufige Prüfung gestellt worden, so sollte der Anmelder in seinem Interesse gleichzeitig mit der Einreichung der Änderungen beim Internationalen Büro auch eine Kopie der Änderungen bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde einreichen (siehe Regel 62.2 a), erster Satz).

### Auswirkungen von Änderungen hinsichtlich der Übersetzung der internationalen Anmeldung beim Eintritt in die nationale Phase

Der Anmelder wird darauf hingewiesen, daß bei Eintritt in die nationale Phase möglicherweise anstatt oder zusätzlich zu der Übersetzung der Ansprüche in der eingereichten Fassung eine Übersetzung der nach Artikel 19 geänderten Ansprüche an die bestimmten/ausgewählten Ämter zu übermitteln ist.

Nähere Einzelheiten über die Erfordernisse jedes bestimmten/ausgewählten Amtes sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT

### INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

<b>Aktenzeichen des Anmelders oder Anwalts</b> <b>98P2821P</b>	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
<b>Internationales Aktenzeichen</b> <b>PCT/DE 99/02844</b>	<b>Internationales Anmeldedatum</b> <i>(Tag/Monat/Jahr)</i> <b>08/09/1999</b>	<b>(Frühestes) Prioritätsdatum (Tag/Monat/Jahr)</b> <b>30/09/1998</b>
<b>Anmelder</b>  <b>SIEMENS AKTIENGESELLSCHAFT et al.</b>		

Dieser internationale Recherchenbericht wurde von der internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

**1. Grundlage des Berichts**

a. Hinsichtlich der Sprache ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

b. Hinsichtlich der in der internationalen Anmeldung offenbarten Nucleotid- und/oder Aminosäuresequenz ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

**4. Hinsichtlich der Bezeichnung der Erfindung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

**5. Hinsichtlich der Zusammenfassung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

☐ wie vom Anmelder vorgeschlagen

☒ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ weil diese Abbildung die Erfindung besser kennzeichnet.

☐ keine der Abb.

**A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**  
IPK 7 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)  
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 752 636 A (SUN MICROSYSTEM) 8. Januar 1997 (1997-01-08) Spalte 3, Zeile 11 - Spalte 4, Zeile 19 Spalte 6, Zeile 35 - Spalte 10, Zeile 37; Ansprüche; Abbildungen 3,5	1-10
A	US 5 611 048 A (JACOBS ET AL.) 11. März 1997 (1997-03-11) Spalte 2, Zeile 1 - Zeile 33 Spalte 5, Zeile 65 - Spalte 11, Zeile 25; Anspruch 1; Abbildungen 5-8	1-10

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen☒ Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche

16. Februar 2000

Absenddatum des internationalen Recherchenberichts

24/02/2000

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Soler, J

**INTERNATIONALER RECHERCHENBERICHT**

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

**PCT/DE 99/02844**

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 752636	A	08-01-1997	US	5734718 A	31-03-1998
			JP	9231174 A	05-09-1997
<hr/>					
US 5611048	A	11-03-1997	KEINE		
<hr/>					

## PATENT COOPERATION TREATY

## PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

RECEIVED

JUL 23 2001

Technology Center 2100

40801  
09/806435  
Translation  
2131

Applicant's or agent's file reference 98P2821P	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE99/02844	International filing date (day/month/year) 08 September 1999 (08.09.99)	Priority date (day/month/year) 30 September 1998 (30.09.98)
International Patent Classification (IPC) or national classification and IPC G06F 1/00		
Applicant SIEMENS AKTIENGESELLSCHAFT		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 2 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 07 March 2000 (07.03.00)	Date of completion of this report 19 January 2001 (19.01.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE99/02844

## I. Basis of the report

## 1. With regard to the elements of the international application:\*

- ☐ the international application as originally filed
- ☒ the description:  
pages \_\_\_\_\_ 1-17 \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☒ the claims:  
pages \_\_\_\_\_ 2-8, 10-12 \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, as amended (together with any statement under Article 19  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_ 1, 9 \_\_\_\_\_, filed with the letter of 30 November 2000 (30.11.2000)
- ☒ the drawings:  
pages \_\_\_\_\_ 1-3 \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the sequence listing part of the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_

## 2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language \_\_\_\_\_ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

## 3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/fig \_\_\_\_\_

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).\*\*

\* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

\*\* Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.  
PCT/DE 99/02844**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement****1. Statement**

Novelty (N)	Claims	2-8, 10-12	YES
	Claims	1, 9	NO
Inventive step (IS)	Claims		YES
	Claims	1-12	NO
Industrial applicability (IA)	Claims	1-12	YES
	Claims		NO

**2. Citations and explanations**

This report makes reference to the following documents:

- D1: HP-UX 11.00 Manual  
([http://www.devresource.hp.com/STK/man/11.00/passwr\\_d\\_1.html](http://www.devresource.hp.com/STK/man/11.00/passwr_d_1.html))
- D2: Deborah Russell, G. T. Gangemi Sr: Computer Security Basics, July 1992, O'Reilly & Associates.

Neither document is cited in the international search report. A copy of document D1 was communicated to the applicant by telephone on 23.11.2000. A copy of D2 is attached to this examination report.

1. The subject matter of the main Claim 1 is not novel, because D1 discloses the following prior art (PCT Article 33(2)):

Features a) - d) describe the typical course of a client/server session: in the claims, the client is referred to as the "first computer", and the server as the "second computer". The client's service request is additionally secured by means of a

password. If the password is valid, the service is carried out, otherwise it is not. This is current practice e.g. in FTP (file transfer protocol) and telnet services. Both services are implemented as standard in Unix, but do not form part of the actual operating system kernel. They are referred to as service programs because they carry out a service (internet service).

Features e) and f) are both apparent in D1. A superuser can cause a password to expire by using the option -x. The first time the service (e.g. FTP or telnet) is used after the expiry of the password, the user is requested to update the password. In order to do this, the operating system invokes passwd [name], with the user ID as parameter. Alternatively, the password can be amended by the server. The advantages and disadvantages of user- and system-generated passwords are generally known, and are discussed, for example, in D2.

2. Main Claim 9 defines the device corresponding to the process Claim 1, and is therefore not novel either (PCT Article 33(2)).
3. Dependent Claims 2-8 and 10-11 define trivial amendments to each of the main claims to which they refer, and cannot be considered inventive (PCT Article 33(3)). The documents cited in the search report disclose numerous devices and methods for the secure transmission of passwords between client and server (authentication, encryption in order to ensure integrity, access controls).



# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE 99/02844

## VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Contrary to PCT Rule 5.1(a)(ii), the description does not cite D1 or indicate the relevant prior art disclosed therein.
2. The description on page 3, line 13 to page 4, line 26 should be brought into line with the amended Claims 1 and 9 (PCT Rule 5.1(a)(iii)).

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.  
PCT/DE 99/02844

## VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. In main Claim 1, line 18 and main Claim 9, line 22, "invalid" should be replaced by "expired". The updating of an invalid password (i.e. a password that had never been valid) would not make sense. This change would have been admissible since it is supported by the original description on page 1, lines 22-29.
2. The features of Claims 1-12 have not been given reference signs enclosed in parentheses (PCT Rule 6.2(b)).

## PCT-ANTRAG

98P2821P

Original (für EINREICHUNG) - gedruckt am 30.08.1999 11:25:49 AM

<b>0</b>	<b>Vom Anmeldeamt auszufüllen</b>	
<b>0-1</b>	Internationales Aktenzeichen.	
<b>0-2</b>	Internationales Anmeldedatum	
<b>0-3</b>	Name des Anmeldeamts und "PCT International Application"	
<b>0-4</b> <b>0-4-1</b>	<b>Formular - PCT/RO/101 PCT-Antrag</b> erstellt durch Benutzung von	<b>PCT-EASY Version 2.84</b> <b>(aktualisiert 01.07.1999)</b>
<b>0-5</b>	<b>Antragssuchen</b> Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird	
<b>0-6</b>	<b>(Vom Anmelder gewähltes) Anmeldeamt</b>	<b>Deutsches Patent- und Markenamt (RO/DE)</b>
<b>0-7</b>	<b>Aktenzeichen des Anmelders oder Anwalts</b>	<b>98P2821P</b>
<b>I</b>	<b>Bezeichnung der Erfindung</b>	<b>VERFAHREN UND ANORDNUNG ZUR AKTUALISIERUNG EINES PASSWORTES</b>
<b>II</b>	<b>Anmelder</b>	
<b>II-1</b>	Diese Person ist	nur Anmelder
<b>II-2</b>	Anmelder für	Alle Bestimmungstaaten mit Ausnahme von US
<b>II-4</b>	Name	SIEMENS AKTIENGESELLSCHAFT
<b>II-5</b>	Anschrift:	Wittelsbacherplatz 2 D-80333 München Deutschland
<b>II-6</b>	Staatsangehörigkeit (Staat)	DE
<b>II-7</b>	Sitz/Wohnsitz (Staat)	DE
<b>II-8</b>	Telefonnr.	(089) 636-82819
<b>II-9</b>	Telefaxnr.	(089) 636-81857
<b>III-1</b>	<b>Anmelder und/oder Erfinder</b>	
<b>III-1-1</b>	Diese Person ist	Anmelder und Erfinder
<b>III-1-2</b>	Anmelder für	Nur US
<b>III-1-4</b>	Name (FAMILIENNAME, Vorname)	FRIES, Steffen
<b>III-1-5</b>	Anschrift:	Wagenbauerstr. 5 D-81677 München Deutschland
<b>III-1-6</b>	Staatsangehörigkeit (Staat)	DE
<b>III-1-7</b>	Sitz/Wohnsitz (Staat)	DE

Wgs

## PCT-ANTRAG

Original (für EINREICHUNG) - gedruckt am 30.08.1999 11:25:49 AM

<b>III-2</b>	<b>Anmelder und/oder Erfinder</b>	<b>Anmelder und Erfinder</b>
III-2-1	Diese Person ist	Nur US
III-2-2	Anmelder für	EUCHNER, Martin
III-2-4	Name (FAMILIENNAME, Vorname)	Lorenzstr. 2
III-2-5	Anschrift:	D-81737 München
		Deutschland
III-2-6	Staatsangehörigkeit (Staat)	DE
III-2-7	Sitz/Wohnsitz (Staat)	DE
<b>IV-1</b>	<b>Anwalt oder gemeinsamer Vertreter; oder besondere Zustellanschrift</b> Die unten bezeichnete Person ist/wird hiermit bestellt, um den (die) Anmelder vor den internationalen Behörden zu vertreten, und zwar als:	<b>gemeinsamer Vertreter</b>
IV-1-1	Name	SIEMENS AKTIENGESELLSCHAFT
IV-1-2	Anschrift:	Postfach 22 16 34
		D-80506 München
		Deutschland
IV-1-3	Telefonnr.	(089) 636-82819
IV-1-4	Telefaxnr.	(089) 636-81857
<b>V</b>	<b>Bestimmung von Staaten</b>	
<b>V-1</b>	Regionales Patent (andere Schutzrechtsarten oder Verfahren sind ggf. in Klammern nach der (den) betreffenden Bestimmung(en) angegeben)	EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE und jeder weitere Staat, der Mitgliedsstaat des Europäischen Patentübereinkommens und Vertragsstaat des PCT ist
<b>V-2</b>	Nationales Patent (andere Schutzrechtsarten oder Verfahren sind ggf. in Klammern nach der (den) betreffenden Bestimmung(en) angegeben)	US
<b>V-5</b>	<b>Erklärung bzgl. vorsorglicher Bestimmungen</b> Zusätzlich zu den unter Punkten V-1, V-2 and V-3 vorgenommenen Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der nachstehend unter Punkt V-6 angegebenen Staaten. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt.	
<b>V-6</b>	<b>Staaten, die von der Erklärung über vorsorgliche Bestimmungen ausgenommen werden</b>	KEINE

## PCT-ANTRAG

Original (für EINREICHUNG) - gedruckt am 30.08.1999 11:25:49 AM

VI-1	<b>Priorität einer früheren nationalen Anmeldung beansprucht</b>		
VI-1-1	Anmeldedatum	30 September 1998 (30.09.1998)	
VI-1-2	Aktenzeichen	198 45 055.9	
VI-1-3	Staat	DE	
VI-2	<b>Ersuchen um Erstellung eines Prioritätsbeleges</b> Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der in der (den) nachstehend genannten Zeile(n) bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln:	VI-1	
VII-1	<b>Gewählte internationale Recherchenbehörde</b>	Europäisches Patentamt (EPA) (ISA/EP)	
VIII	<b>Kontrollliste</b>	Anzahl der Blätter	Elektronische Datei(en) beigefügt
VIII-1	Antrag	4	-
VIII-2	Beschreibung	17	-
VIII-3	Ansprüche	4	-
VIII-4	Zusammenfassung	1	98 p 2821 p.txt
VIII-5	Zeichnung(en)	8 3	-
VIII-7	INSGESAMT	28 29	8.9 9.
	<b>Beigefügte Unterlagen</b>	Unterlage(n) in Papierform beigefügt	Elektronische Datei(en) beigefügt
VIII-8	Blatt für die Gebührenberechnung	✓	-
VIII-16	PCT-EASY-Diskette	-	Diskette
VIII-17	Sonstige (einzeln aufgeführt):	Kopie der Ursprungsfassung	-
VIII-18	Nr. der Abb. der Zeichn., die mit der Zusammenf. veröffentlicht werden soll	-	
VIII-19	<b>Sprache der int. Anmeldung</b>	Deutsch	
IX-1	<b>Unterschrift des Anmelders oder Anwalts</b>	<i>i.V. Marg</i>	
IX-1-1	Name	SIEMENS AKTIENGESELLSCHAFT	
IX-1-2	Name der unterzeichnenden Person	Margraf	
IX-1-3	Eigenschaft	Nr. 144/74 Ang-AV	
IX-2	<b>Unterschrift des Anmelders oder Anwalts</b>		
IX-2-1	Name (FAMILIENNAME, Vorname)	FRIES, Steffen	
IX-3	<b>Unterschrift des Anmelders oder Anwalts</b>		
IX-3-1	Name (FAMILIENNAME, Vorname)	EUCHNER, Martin	

## VOM ANMELDEAMT AUSZUFÜLLEN

10-1	<b>Datum des tatsächlichen Eingangs dieser internationalen Anmeldung</b>	
------	--------------------------------------------------------------------------	--

## PCT-ANTRAG

Original (für EINREICHUNG) - gedruckt am 30.08.1999 11:25:49 AM

VI-1	<b>Priorität einer früheren nationalen Anmeldung beansprucht</b>		
VI-1-1	Anmeldedatum	30 September 1998 (30.09.1998)	
VI-1-2	Aktenzeichen	198 45 055.9	
VI-1-3	Staat	DE	
VI-2	<b>Ersuchen um Erstellung eines Prioritätsbeleges</b> Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der in der (den) nachstehend genannten Zeile(n) bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln:	VI-1	
VII-1	<b>Gewählte internationale Recherchenbehörde</b>	Europäisches Patentamt (EPA) (ISA/EP)	
VIII	<b>Kontrollliste</b>	Anzahl der Blätter	Elektronische Datei(en) beigelegt
VIII-1	Antrag	4	-
VIII-2	Beschreibung	17	-
VIII-3	Ansprüche	4	-
VIII-4	Zusammenfassung	1	98_p_2821_p.txt
VIII-5	Zeichnung(en)	23	-
VIII-7	INSGESAMT	2829	
	<b>Beigelegte Unterlagen</b>	Unterlage(n) in Papierform beigelegt	Elektronische Datei(en) beigelegt
VIII-8	Blatt für die Gebührenberechnung	✓	-
VIII-16	PCT-EASY-Diskette	-	Diskette
VIII-17	Sonstige (einzeln aufgeführt):	Kopie der Ursprungsfassung	-
VIII-18	Nr. der Abb. der Zeichn., die mit der Zusammenf. veröffentlicht werden soll	-	
VIII-19	Sprache der int. Anmeldung	Deutsch	
IX-1	<b>Unterschrift des Anmelders oder Anwalts</b>	<i>i. V. Marg</i>	
IX-1-1	Name	SIEMENS AKTIENGESELLSCHAFT	
IX-1-2	Name der unterzeichnenden Person	Margraf	
IX-1-3	Eigenschaft	Nr. 144/74 Ang-AV	
IX-2	<b>Unterschrift des Anmelders oder Anwalts</b>	<i>Steffen Fries</i>	
IX-2-1	Name (FAMILIENNAME, Vorname)	FRIES, Steffen	
IX-3	<b>Unterschrift des Anmelders oder Anwalts</b>	<i>Martin Euchner</i>	
IX-3-1	Name (FAMILIENNAME, Vorname)	EUCHNER, Martin	

## VOM ANMELDEAMT AUSZUFÜLLEN

10-1	<b>Datum des tatsächlichen Eingangs dieser internationalen Anmeldung</b>	
------	--------------------------------------------------------------------------	--

**PCT-ANTRAG**

98P2821P

Original (für EINREICHUNG) - gedruckt am 30.08.1999 11:25:49 AM

10-2	<b>Zeichnung(en):</b>	
10-2-1	Eingegangen	
10-2-2	Nicht eingegangen	
10-3	<b>Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingeg. Unterlage(n) oder Zeichnung(en) zur Vervollständigung dieser int. Anmeldung</b>	
10-4	<b>Datum des fristgerechten Eingangs der Berichtigung nach PCT Artikel 11(2)</b>	
10-5	<b>Internationale Recherchenbehörde</b>	ISA/EP
10-6	<b>Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchegebühr aufgeschoben</b>	

**VOM INTERNATIONALEN BÜRO AUSZUFÜLLEN**

11-1	<b>Datum des Eingangs des Aktenexemplars beim Internationalen Büro</b>	
------	------------------------------------------------------------------------	--

**PCT (ANHANG - BLATT FÜR DIE  
GEBÜHRENBERECHNUNG)**

98P2821P

Original (für EINREICHUNG) - gedruckt am 30.08.1999 11:25:49 AM

(Dieses Blatt ist nicht Teil und zählt nicht als Blatt der internationalen Anmeldung)

<b>0</b>	<b>Vom Anmeldeamt auszufüllen</b>		
0-1	Internationales Aktenzeichen.		
0-2	Eingangsstempel des Anmeldeamts		
<b>0-4</b>	<b>Formular - PCT/RO/101 (Anlage)</b>		
0-4-1	PCT Blatt für die Gebührenberechnung erstellt durch Benutzung von	<b>PCT-EASY Version 2.84 (aktualisiert 01.07.1999)</b>	
0-9	Aktenzeichen des Anmelders oder Anwalts	<b>98P2821P</b>	
<b>2</b>	<b>Anmelder</b>	<b>SIEMENS AKTIENGESELLSCHAFT, et al.</b>	
<b>12</b>	<b>Berechnung der vorgeschriebenen Gebühren</b>	<b>Höhe der Gebühr/Multiplikator</b>	<b>Gesamtbeträge (DEM)</b>
12-1	Übermittlungsgebühr <b>T</b>	⇒	<b>150</b>
12-2	Recherchegebühr <b>S</b>	⇒	<b>1.848,26</b>
12-3	Internationale Gebühr Grundgebühr (erste 30 Blätter) <b>b1</b>	<b>807,76</b>	
12-4	Anzahl der Blätter über 30	<b>0</b>	
12-5	Zusatzblattgebühr <b>(X)</b>	<b>19,56</b>	
12-6	Gesamtbetrag der weiteren Gebühren <b>b2</b>	<b>0</b>	
12-7	<b>b1 + b2 =</b> <b>B</b>	<b>807,76</b>	
12-8	Bestimmungsgebühren Anzahl der in der internationalen Anmeldung vorgenommenen Bestimmungen	<b>2</b>	
12-9	Anzahl der zu zahlenden Bestimmungsgebühren (höchstens 10)	<b>2</b>	
12-10	Bestimmungsgebühr <b>(X)</b>	<b>185,8</b>	
12-11	Gesamtbetrag der Bestimmungsgebühren <b>D</b>	<b>371,6</b>	
12-12	PCT-EASY-Gebührenermäßigung <b>R</b>	<b>-248,39</b>	
12-13	Gesamtbetrag der internationalen Gebühr (B+D+R) <b>I</b>	⇒	<b>930,97</b>
12-14	Gebühr für Prioritätsbeleg Anzahl der beantragten Prioritätsbelege	<b>1</b>	
12-15	Gebühr per Prioritätsbeleg <b>(X)</b>	<b>35</b>	
12-16	Gesamtbetrag Gebühr für Prioritätsbeleg(e) <b>P</b>	⇒	<b>35</b>
<b>12-17</b>	<b>GESAMTBETRAG DER ZU ZAHLENDEN GEBÜHREN (T+S+I+P)</b>	⇒	<b>2.964,23</b>
<b>12-19</b>	<b>Zahlungsart</b>	<b>Sonstige: Abbuchung durch gesonderte Zahlungsliste</b>	



**PCT (ANHANG - BLATT FÜR DIE  
GEBÜHRENBERECHNUNG)**

Original (für EINREICHUNG) - gedruckt am 30.08.1999 11:25:49 AM

12-20	Anweisungen betreffend laufendes Konto Das Anmeldeamt:	Deutsches Patent- und Markenamt (RO/DE)
12-20-2	wird beauftragt, Fehlbeträge oder Überzahlungen des vorstehend angegebenen Gesamtbetrags der Gebühren meinem laufenden Konto zu belasten bzw. gutzuschreiben	✓
12-21	Nummer des laufenden Kontos	409022601
12-22	Datum	30 August 1999 (30.08.1999)
12-23	Name und Unterschrift	SIEMENS AKTIENGESELLSCHAFT <i>i. V. Merg</i>

**PRÜFPROTOKOLL UND BEMERKUNGEN**

13-2-2	Prüfergebnisse Staaten	Grün? Es können mehr Bestimmungen vorgenommen werden. Bitte überprüfen.
--------	------------------------	----------------------------------------------------------------------------

**Beschreibung****Verfahren und Anordnung zur Aktualisierung eines Paßwortes**

- 5 Die Erfindung betrifft ein Verfahren und eine Anordnung zur Aktualisierung eines Paßwortes.

Aus [1] sind ein solches Verfahren und eine solche Anordnung bekannt.

10

- Bei einer solchen Anordnung ist für den Fall, daß ein Benutzer diese Anordnung benutzen will, vorgesehen, daß von dem Benutzer eine Eingabe eines Paßwortes in die Anordnung gefordert wird. Nach Eingabe des Paßwortes durch den Benutzer wird  
15 von der Anordnung anhand einer Datenbank überprüft, ob eine eingegebene Paßwortangabe für den Benutzer ein gültiges Paßwort ist oder nicht.

- In der Datenbank der Anordnung ist eine Liste mit zulässigen Benutzern der Anordnung gespeichert. Jedem Benutzer ist jeweils ein Paßwort zugeordnet, welches gespeichert ist und mit dem das eingegebene Paßwort verglichen wird. Jedem Paßwort ist ferner eine Zeitangabe zugeordnet. Mit der Zeitangabe wird angegeben, für welchen Zeitraum das Paßwort gültig sein  
20 soll. Ist der Zeitraum abgelaufen, so wird das gespeicherte Paßwort ungültig und der Benutzer wird zu einer Aktualisierung des Paßwortes aufgefordert, wenn er die Benutzung der Anordnung aufnehmen will.

- 30 Auf diese Weise wird eine gewisse, von dem jeweiligen Zeitraum abhängige Aktualität des jeweiligen Paßwortes erreicht, wodurch ein höherer Sicherheitsgrad für die Anordnung hinsichtlich eines Mißbrauchs bzw. eines unbefugten Ermitteln eines Paßworts gewährleistet wird. Ferner ist aus [1] bekannt, daß die Paßwortangabe in der Datenbank in kryptierter Form (verschlüsselt oder gebildet unter Verwendung einer Einweg-Hashfunktion) abgelegt werden kann. Aus [1] ist weiterhin  
35

bekannt, daß die Paßwortangabe kryptiert über eine Kommunikationsverbindung transportiert werden kann. Ein Beispiel dafür ist das Domain Logon bei Windows NT. Der Zeitpunkt des Paßwortwechsels ist jedoch auf den Zeitpunkt der Login-Prozedur  
5 beschränkt.

Aus [2] ist ein Kommunikationsstandard, der H.235-Standard, bekannt, in dem Rahmenbedingungen, insbesondere Formate von Nachrichten, die zwischen miteinander verbundenen Rechnern im  
10 Rahmen einer multimedialen Kommunikation ausgetauscht werden können.

Die Rechner können logisch oder fest miteinander verbunden sein.  
15

Ein Nachteil der aus [2] bekannten Verfahren ist insbesondere darin zu sehen, daß lediglich statische Paßworte für einen Benutzer eingesetzt werden können, wodurch die Wahrscheinlichkeit relativ hoch ist, daß in den Rechnern gespeicherte  
20 Paßworte irgendwann von einem unbefugten Dritten, einem Angreifer, ermittelt und mißbraucht werden können, wodurch die Sicherheit der einzelnen Rechner nicht mehr gewährleistet ist.

25 Aus [3] ist ein weiterer Kommunikationsstandard, der H.225-Standard, bekannt.

Aus [4] ist die sogenannte Abstract Syntax Notation 1 (ASN.1) beschrieben, die zur Definition des Formats einer Nachricht verwendet wird, die zur Definition des Formats einer Nachricht im Sinne der aus [2] und [3] bekannten Standards verwendet wird.  
30

Eine Übersicht über Protokolle zur Aktualisierung kryptographischer Schlüssel ist in [5] zu finden.  
35

Insbesondere bei einem großen Kommunikationsnetz mit einer Vielzahl miteinander verbundenen Rechnern, beispielsweise dem Internet, stellt die oben beschriebene Situation ein hohes Risiko dar.

5

Somit liegt der Erfindung das Problem zugrunde, ein Verfahren und eine Anordnung zur Aktualisierung eines Paßwortes zwischen zwei miteinander verbundenen Rechnern anzugeben.

10 Das Problem wird durch die Anordnung sowie das Verfahren mit den Merkmalen gemäß den unabhängigen Ansprüchen gelöst.

Ein Verfahren zur Aktualisierung eines Paßwortes zwischen einem ersten Rechner und einem zweiten Rechner, weist folgende Schritte auf:

15

a) der zweite Rechner empfängt im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht, wobei die Dienstanforderungsnachricht das Paßwort aufweist,

20

b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,

c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,

25

d) für den Fall, daß das Paßwort gültig ist, wird der Dienst erbracht,

e) für den Fall, daß das Paßwort ungültig ist, wird von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet, mit der eine Aktualisierung des Paßworts gefordert wird, und

30

f) von dem ersten Rechner und/oder dem zweiten Rechner wird ein aktualisiertes Paßwort gebildet wird, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

35

Eine Anordnung weist mindestens einen ersten Rechner und mindestens einen zweiten Rechner auf zur Aktualisierung eines Paßwortes zwischen den Rechnern,

wobei der erste Rechner und der zweite Rechner jeweils einen Prozessor aufweisen, die derart eingerichtet sind, daß folgende Schritte durchführbar sind:

- a) der zweite Rechner empfängt im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht, wobei die Dienstanforderungsnachricht das Paßwort aufweist,
- b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,
- c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,
- d) für den Fall, daß das Paßwort gültig ist, wird der Dienst erbracht,
- e) für den Fall, daß das Paßwort ungültig ist, wird von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet, mit der eine Aktualisierung des Paßworts gefordert wird, und
- f) von dem ersten Rechner und/oder dem zweiten Rechner wird ein aktualisiertes Paßwort gebildet, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

Durch die Erfindung wird eine Aktualisierung eines Paßwortes zwischen zwei Rechnern während einer zwischen den beiden Rechnern bestehenden Kommunikationsverbindung möglich. Der zweite Rechner kann den ersten Rechner anschaulich dazu zwingen, daß der erste Rechner das Paßwort zu aktualisieren hat, wenn der erste Rechner einen Dienst von dem zweiten Rechner anfordert. Damit gewährleistet der zweite Rechner die Aktualität der Paßworte, wodurch die Sicherheit der Kommunikation zwischen den Rechnern erhöht wird.

Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

- Die im weiteren beschriebenen Weiterbildungen gelten sowohl für das Verfahren als auch die Anordnung, wobei bei der Weiterbildung der Anordnung jeweils die Prozessoren der Rechner derart eingerichtet sind, daß die Weiterbildung realisierbar ist.
- Die Bildung des aktualisierten Paßwortes erfolgt in einer Weiterbildung auf folgende Weise:
- a) der erste Rechner sendet eine Paßwortnachricht zu dem zweiten Rechner, in der das aktualisierte Paßwort enthalten ist in einer Weise, daß das aktualisierte Paßwort nur unter Verwendung des Paßwortes ermittelt werden kann,
  - b) der zweite Rechner ermittelt unter Verwendung des Paßwortes das aktualisierte Paßwort aus der Paßwortnachricht,
  - c) der zweite Rechner speichert das aktualisierte Paßwort.
- Der zweite Rechner kann eine Bestätigungsnachricht senden, mit der der Einsatz des aktualisierten Paßwortes im Rahmen der Kommunikationsverbindung bestätigt wird.
- Zu Beginn des Verfahrens wird vorzugsweise der erste Rechner durch den zweiten Rechner authentifiziert unter Verwendung einer in der Dienstanforderungsnachricht enthaltenen Authentifikationsangabe des ersten Rechners. Damit wird das Sicherheitsniveau der jeweiligen Kommunikationsverbindung erhöht.
- Die Überprüfung, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist, erfolgt in einer weiteren Ausgestaltung anhand einer Kontrolldatenbank, in der für den ersten Rechner angegeben ist, ob zuvor schon von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet worden ist. Durch diese Vereinfachung wird das Verfahren schneller durchführbar, da eine

erhebliche Rechenzeiteinsparung im Rahmen der Überprüfung erreicht wird.

5 In der Dienstanforderungsnachricht ist bevorzugt eine Angabe  
enthalten zur Integritätssicherung der Dienstanforderungs-  
nachricht, mit welcher Angabe von dem zweiten Rechner die  
empfangene Dienstanforderungsnachricht auf ihre Integrität  
hin überprüft wird. Nur für den Fall, daß die Integrität der  
Dienstanforderungsnachricht gewährleistet ist, wird das Ver-  
10 fahren durchgeführt; sonst wird der angeforderte Dienst zu-  
rückgewiesen. Damit wird das Sicherheitsniveau der jeweiligen  
Kommunikationsverbindung weiter erhöht.

15 In der Paßwortnachricht ist das aktualisierte Paßwort bevor-  
zugt verschlüsselt enthalten, wobei der Schlüssel zur Ver-  
schlüsselung des aktualisierten Paßwortes abhängig von dem  
Paßwort gebildet wird. Durch diese Weiterbildung wird ein Zu-  
sammenhang zwischen dem „alten“ Paßwort und dem aktualisier-  
ten Paßwort geschaffen, womit nur der Besitzer des Paßwortes  
20 das aktualisierte Paßwort überhaupt ermitteln kann. Damit  
wird der Schutz des aktualisierten Paßwortes bei dessen Über-  
tragung verbessert.

25 Der Schlüssel wird bevorzugt durch mehrfache Aneinanderrei-  
hung des Paßwortes gebildet.

Es sind vorzugsweise mehrere erste Rechner vorgesehen, die  
jeweils ein Paßwort gemeinsam mit dem zweiten Rechner besit-  
zen, wobei das Paßwort jeweils eindeutig ist für die Kommuni-  
30 kationsverbindung zwischen dem jeweiligen ersten Rechner und  
dem zweiten Rechner. Damit ist die Erfindung sehr gut ein-  
setzbar in einem großen Kommunikationsnetz, in dem ein Ser-  
ver, der zweite Rechner, mehreren Clients, den ersten Rech-  
nern, Dienste über das Kommunikationsnetz anbietet.

35

Ferner können mehrere zweite Rechnern vorgesehen sein, die  
jeweils ein Paßwort gemeinsam mit jedem ersten Rechner besit-

zen, wobei das Paßwort jeweils eindeutig ist für die Kommunikationsverbindung zwischen dem jeweiligen zweiten Rechner und dem jeweiligen zweiten Rechner.

- 5 Ein Ausführungsbeispiel der Erfindung ist in den Figuren dargestellt und wird im weiteren näher erläutert:

Es zeigen

- 10 Figur 1 ein Ablaufdiagramm, in dem die Verfahrensschritte des Ausführungsbeispiels dargestellt sind;

- Figur 2 eine Skizze, in der Rechner dargestellt sind, die über ein Kommunikationsnetz miteinander verbunden  
15 sind.

- Fig.2** zeigt einen ersten Rechner 200 mit einem Speicher 202 und einem Prozessor 203, die jeweils über einen Bus 204 miteinander und mit einer Eingangs-/Ausgangsschnittstelle 201  
20 verbunden sind.

- Über die Eingangs-/Ausgangsschnittstelle 201 ist der erste Rechner 200 mit einem Bildschirm 205, einer Tastatur 206 sowie einer Computermouse 207 verbunden.  
25

- Ferner ist der erste Rechner 200 über ein Kommunikationsnetz 260, in dem Beispiel ein ISDN-Netz (Integrated Services Digital Network) mit weiteren Rechnern 210, 220, 230, 240 und 250 verbunden.  
30

- In dem ersten Rechner 200 ist eine Datenbank 208 gespeichert.

- Die weiteren Rechner 210, 220, 230, 240 und 250 weisen jeweils ebenfalls einen Prozessor 213, 223, 233, 243 und 253 sowie jeweils einen Speicher 212, 222, 232, 242 und 252 auf.  
35 Jeweils der Prozessor 213, 223, 233, 243 und 253 und der Speicher 212, 222, 232, 242 und 252 sind über jeweils einen



Bus 214, 224, 234, 244 und 254 über eine Eingangs-  
/Ausgangsschnittstelle 211, 221, 231, 241 und 251 mit dem  
Kommunikationsnetz 260 verbunden. Ferner sind die weiteren  
Rechner 210, 220, 230, 240 und 250 jeweils mit einem Bild-  
5 schirm 215, 225, 235, 245 und 255 sowie einer Tastatur 216,  
226, 236, 246 und 256 sowie einer Computermouse 217, 227, 237,  
247 und 257 verbunden.

Zwischen den Rechnern 200, 210, 220, 230, 240 und 250 erfolgt  
10 die Kommunikation, d.h. ein gesicherter Austausch multimedia-  
ler Daten, gemäß dem H.235-Standard, wie in [2] beschrieben.

Der erste Rechner 200 ist als ein Server ausgestaltet und  
stellt den weiteren Rechnern 210, 220, 230, 240 und 250 ver-  
15 schiedene Dienste zur Verfügung.

Im weiteren wird angenommen, daß ein zweiter Rechner 210 ei-  
nen Dienst von dem ersten Rechner 200 in Anspruch nehmen  
will.

20

Zu Beginn des Verfahrens wird eine Kommunikationsverbindung  
zwischen dem zweiten Rechner 210 und dem ersten Rechner 200  
gemäß den in [2] und [3] beschriebenen Verfahren aufgebaut.  
Nach erfolgter Initialisierung der Kommunikationsverbindung  
25 besteht zwischen dem zweiten Rechner 210 und dem ersten Rech-  
ner 200 eine logische Verbindung, d.h. der Kommunikationsver-  
bindung ist ein logischer Kanal zugeordnet, der eindeutig  
identifizierbar ist. Über den logischen Kanal werden zwischen  
den Rechnern 200, 210, 220, 230, 240, 250 Nachrichten 270,  
30 280 ausgetauscht.

Ist die Kommunikationsverbindung aufgebaut, kann durch den  
zweiten Rechner 210 von dem ersten Rechner 200 ein Dienst in  
Anspruch genommen, in diesem Fall eine Datenbankabfrage von  
35 einer in dem ersten Rechner 200 gespeicherten Datenbank 208.

Im weiteren wird das Verfahren beschrieben, das durchgeführt wird, wenn der zweite Rechner 210 von dem ersten Rechner 200 Daten aus dessen Datenbank 208 ermitteln möchte.

- 5 Die gewünschten Kriterien für die Datenbankabfrage werden von einem Benutzer des zweiten Rechners 210 in den zweiten Rechner 210 eingegeben. Von dem zweiten Rechner 210 wird eine Dienstanforderungsnachricht 101 gebildet (Schritt 100), in der die Kriterien für die Datenbankabfrage enthalten sind  
10 (vgl. **Fig.1**).

Ferner sind in der Dienstanforderungsnachricht 101 folgende Größen enthalten:

- eine Authentifikationsangabe (Authentication Token), mit  
15 der eine Authentifikation des zweiten Rechners 210 durch den ersten Rechner 200 möglich ist; die Authentifikationsangabe erlaubt die Darstellung des Paßwortes in verschiedener Form (beispielsweise verschlüsselt oder gebildet unter Verwendung einer Einweg-Hashfunktion als Einweg-Hashwert);
- 20 - eine H.235-Adresse, mit der der erste Rechner 200 eindeutig identifiziert wird;
- eine Paßwortangabe PW des Benutzers des zweiten Rechners 210.

- 25 In dem ersten Rechner 200 ist für jeden weiteren Rechner 210, 220, 230, 240 und 250 ein dem jeweiligen Rechner 210, 220, 230, 240 und 250 zugeordnetes Paßwort gespeichert. Ist in einer Dienstanforderungsnachricht 101, die von einem weiteren Rechner 210, 220, 230, 240 und 250 gebildet wird, eine Paßwortangabe enthalten, die gleich dem gespeicherten Paßwort  
30 für den weiteren Rechner 210, 220, 230, 240 und 250 ist, so wird der angeforderte Dienst dem Benutzer gewährt, d.h. von dem ersten Rechner 200 ausgeführt.

- 35 Dem Paßwort ist jeweils eine erste Zeitangabe t1 zugeordnet, mit der angegeben wird, zu welchem Zeitpunkt das Paßwort gebildet worden ist. Ferner ist dem Paßwort jeweils eine zweite

10

Zeitangabe  $t_2$  zugeordnet, mit der angegeben wird, für welchen Zeitraum das Paßwort gültig ist.

Die Dienstanforderungsnachricht 101 wird von dem zweiten  
5 Rechner 210 an den ersten Rechner 200 übertragen  
(Schritt 102).

Nach Empfang der Dienstanforderungsnachricht 101 in dem er-  
sten Rechner 200 (Schritt 103) wird der zweite Rechner 210  
10 unter Verwendung der Authentifikationsangabe in der Dienstan-  
forderungsnachricht 101 authentifiziert (Schritt 104).

Nach positiver Authentifikation des zweiten Rechners 210 wird  
in einem weiteren Schritt (Schritt 105) die Paßwortangabe PW  
15 aus der Authentifikationsangabe der Dienstanforderungsnach-  
richt 101 ermittelt und die Paßwortangabe wird mit dem in dem  
ersten Rechner 200 gespeicherten Paßwort, welches dem zweiten  
Rechner 200 zugeordnet ist, verglichen (Schritt 106).

20 Bei negativer Authentifikation wird die Dienstanforderungs-  
nachricht 101 verworfen (Schritt 110) und der angeforderte  
Dienst wird nicht ausgeführt.

Stimmen die Paßwortangabe PW und das dem zweiten Rechner 200  
25 zugeordnete Paßwort überein, so wird überprüft, ob das Paß-  
wort gültig ist (Schritt 107). Dies erfolgt in der Weise, daß  
eine aktuelle Zeit  $t_3$ , zu der die Dienstanforderungsnachricht  
101 von dem ersten Rechner 200 empfangen worden ist, ermit-  
telt wird.

30

Stimmen die Paßwortangabe PW und das dem zweiten Rechner 200  
zugeordnete Paßwort überein, so wird die Dienstanforderungs-  
nachricht 101 verworfen (Schritt 115) und der angeforderte  
Dienst wird nicht ausgeführt.

35

Es wird überprüft, ob die aktuelle Zeit  $t_3$  kleiner oder gleich ist der Summe aus der ersten Zeitangabe  $t_1$  und der zweiten Zeitangabe  $t_2$ , also ob gilt:

$$5 \quad t_3 \leq t_1 + t_2. \quad (1)$$

Ist Vorschrift (1) erfüllt, so bedeutet dies, daß die Paßwortangabe dem Paßwort entspricht und das Paßwort noch gültig ist.

10

In diesem Fall wird der mit der Dienstanforderung 101 angeforderte Dienst, also die Datenbankabfrage von dem ersten Rechner 200 durchgeführt (Schritt 108) und das Ergebnis der Datenbankabfrage wird in einer gebildeten Ergebnismeldung  
15 116 (Schritt 109) an den zweiten Rechner 210 übertragen (Schritt 110), in dem das Ergebnis der Datenbankabfrage weiterverarbeitet wird (Schritt 111).

Ist Vorschrift (1) nicht erfüllt, so bedeutet dies, daß zwar  
20 der zweite Rechner 210 aufgrund der erfolgten Authentifikation grundsätzlich zur Anforderung des Dienstes berechtigt ist, das dem zweiten Rechner 210 zugeordnete Paßwort nicht mehr gültig ist.

25 In einem weiteren Schritt (Schritt 120) wird bei ungültigem Paßwort von dem ersten Rechner 200 eine Aktualisierungsmeldung 121 gebildet und an den zweiten Rechner 210 gesendet (Schritt 122), mit der eine Aktualisierung des Paßworts gefordert wird. Ferner wird von dem ersten Rechner 200 in einer  
30 Kontrolldatenbank ein Bit (Kontrollwert) auf einen ersten Wert gesetzt, mit dem angegeben wird, daß das jeweilige Paßwort ungültig ist und die entsprechende Aktualisierungsmeldung 121 an den zweiten Rechner 210 gesendet worden ist.

35 Nach Empfang der Aktualisierungsmeldung 121 (Schritt 123) wird von dem zweiten Rechner ein aktualisiertes Paßwort  $a_{PW}$  gebildet (Schritt 124).

Hält sich der zweite Rechner 210 nicht an die vorgeschriebene Prozedur und generiert erneut eine Dienstanforderung, ohne das Paßwort zu ändern, so kann der erste Rechner 200 dies  
5 nach der Authentifikation des zweiten Rechners 210 und dem Überprüfen des Kontrollwertes feststellen. Ist der Kontrollwert auf den ersten Wert gesetzt, so kann das Verfahren beendet werden (Schritt 131).

10 Das aktualisierte Paßwort aPW wird symmetrisch gemäß dem Data Encryption Standard (DES) verschlüsselt. Als Schlüssel wird das Paßwort PW, welches auch in dem zweiten Rechner 210 bekannt und gespeichert ist, zur Verschlüsselung des aktualisierten Paßworts aPW verwendet.

15 Das verschlüsselte aktualisierte Paßwort aPW wird in einer von dem zweiten Rechner 210 gebildeten Paßwortnachricht 125 (Schritt 126) an den ersten Rechner übertragen (Schritt 127).

20 In der Paßwortnachricht 125 ist eine Integritätsangabe enthalten, mit der die Integrität der Paßwortnachricht 125 überprüft werden kann.

Nach Empfang der Paßwortnachricht 125 (Schritt 128) wird die  
25 Integrität der Paßwortnachricht 125 überprüft (Schritt 129).

Bei negativer Integritätsprüfung wird die Paßwortnachricht 125 verworfen (Schritt 130) und das Verfahren beendet (Schritt 131).

30 Bei positiver Integritätsprüfung wird von dem ersten Rechner 200 das verschlüsselte aktualisierte Paßwort aPW ermittelt (Schritt 132) und das aktualisierte Paßwort aPW wird entschlüsselt (Schritt 133).

35 Das ermittelte aktualisierte Paßwort aPW wird in einem weiteren Schritt als neues Paßwort für den zweiten Rechner 210 ge-

speichert (Schritt 134). Ferner wird von dem ersten Rechner 200 in der Kontrolldatenbank der entsprechende Kontrollwert auf einen zweiten Wert gesetzt, mit dem angegeben wird, daß das jeweilige Paßwort gültig ist.

5

Anschließend wird von dem ersten Rechner 200 eine Bestätigungsnachricht 135 gebildet (Schritt 136) und an den zweiten Rechner 210 übertragen (Schritt 137) und von dem zweiten Rechner 210 empfangen (Schritt 138). Mit der Bestätigungsnachricht 135 wird dem zweiten Rechner 210 der weitere Einsatz des aktualisierten Paßwortes aPW im Rahmen der Kommunikationsverbindung bestätigt.

15

Weiterhin wird von dem ersten Rechner 200 der Dienst erbracht (Schritt 108), die Ergebnismnachricht 116 gebildet (Schritt 109) und die Ergebnismnachricht 116 an den zweiten Rechner 210 übertragen (Schritt 110). In dem zweiten Rechner 210 wird die Ergebnismnachricht 116 weiterverarbeitet (Schritt 111).

20

Ferner wird von dem ersten Rechner 200 in der Kontrolldatenbank das entsprechende Bit auf einen zweiten Wert gesetzt, mit dem angegeben wird, daß das jeweilige Paßwort gültig ist.

25

Bei einer weiteren empfangenen Dienstanforderungsnachricht wird jeweils nach deren Empfang von dem ersten Rechner 200 anhand der Kontrolldatenbank überprüft, ob das jeweilige Paßwort gültig ist oder nicht. Auf diese Weise wird eine sehr schnelle Prüfung des Paßwortes erreicht.

30

Die im Rahmen dieses Verfahrens verwendeten Nachrichten sind gemäß dem H.225.0-Standard, wie er in [3] beschrieben ist, codiert.

35

Zur Definition des im weiteren beschriebenen Formats der einzelnen Nachrichten wird die in [4] beschriebene Abstract Syntax Notation 1 (ASN.1) verwendet.

Die Nachrichten werden als eine in [3] vorgesehene NonStandardMessage codiert, wie im folgenden beschrieben:

```

5  NonStandardMessage ::= SEQUENCE
   {
       requestSeqNum      RequestSeqNum,
       nonStandardData    NonStandardParameter,
       ...
10  tokens                SEQUENCE OF ClearToken OPTIONAL,
       cryptoTokens       SEQUENCE OF CryptoH323Token OPTIONAL,
       integrityCheckValue ICV OPTIONAL
   }

15  NonStandardParameter ::= SEQUENCE
   {
       nonStandardIdentifier NonStandardIdentifier,
       data                  OCTET STRING
20  }

NonStandardIdentifier ::= CHOICE
   {
25  object                OBJECT IDENTIFIER,
       h221NonStandard    H221NonStandard,
       ...
   }

30  data ::= SEQUENCE
   {
       alias              GatekeeperIdentifier,
       confirm             boolean,
35  -- optionally for the provision of integrity
       rejectReason       PWUpdateRejectReason OPTIONAL,
       hash_algorithm      NonIsoIntegrityMechanism OPTIONAL,
       token               HASHED OPTIONAL,
40  -- < alias, confirmation, new password>
       ...
   }

45  PWUpdateRejectReason ::= CHOICE
   {
       notregistered      NULL, -- keep the old password
       pw_wrong            NULL, -- keep the old password
50  pw_old                NULL, -- keep the old password
       ...
   }

```

15

```

NonIsoIntegrityMechanism ::= CHOICE
{
  -- HMAC mechanism used, no truncation, tagging may bei dem
  necessary!
  5   HMAC-MD5          NULL,
      HMAC-iso10118-2-s EncryptIntAlg,
      -- according to ISO/IEC 10118-2 using
      -- EncryptIntAlg as core block encryption algorithm
      -- (short MAC)
  10   HMAC-iso10118-2-1 EncryptIntAlg,
      -- according to ISO/IEC 10118-2 using
      -- EncryptIntAlg as core block encryption algorithm
      -- (long MAC)
      HMAC-iso10118-3  OBJECT IDENTIFIER,
  15   -- according to ISO/IEC 10118-3 using
      -- OID as hash function (OID is SHA-1, RIPE-MD160,
      -- RIPE-MD128)
      ...
}

20
EncryptIntAlg ::= CHOICE
{
  -- core encryption algorithms for RAS message integrity
  nonStandard      NonStandardParameter,
  isoAlgorithm      OBJECT IDENTIFIER,      -- defined in
  25 ISO/IEC 9979
      ...
}

30
AliasAddress ::= CHOICE
{
  e164      IA5String (SIZE (1..128)) (FROM („0123456789#*,“)),
  h323-ID    BMPString (SIZE (1..256)),
              -- Basic ISO/IEC 10646-1 (Unicode)
  35   ...,
  url-ID     IA5String (SIZE (1..512)),
              -- URL style address
  transportID TransportAddress,
  email-ID   IA5String (SIZE (1..512)),
  40   -- rfc822-compliant email address
  partyNumber PartyNumber
}

```

Im weiteren sid einige Alternativen zu dem oben beschriebenen  
 45 Ausführungsbeispiel dargestellt:

Die Art der Integritätssicherung ist grundsätzlich beliebig,  
 ebenso wie der Verschlüsselungsalgorithmus zur Verschlüsse-  
 lung des aktualisierten Paßwortes.

50

Die Realisierung der Nachrichten als Non Standard Messages  
 bzw. Non Standard Data Field ist nicht zwingend notwendig.  
 Die Darstellung der Nachrichten läßt sich auch über neu zu



definierende Nachrichten oder Protokollfelder in den aus [2] und [3] bekannten Standards realisieren.

5 Auch sind das Verfahren und die Anordnung nicht auf die aus [2] und [3] bekannten Standards beschränkt.

Die Bildung der Dienstanforderungsnachricht und/oder der Aktualisierungsnachricht und/oder der Paßwortnachricht und/oder der Bestätigungsnachricht können separat als eigenständige  
10 Nachrichten erfolgen und zwischen den beteiligten Rechnern separat übertragen werden. Es ist ferner in einer Variante möglich, die jeweilige Nachricht gemäß dem Prinzip des sogenannten "Piggybacks" gemeinsam mit anderen Nachrichten zwischen den beteiligten Rechnern zu übertragen.

15

Auch kann der zweite Rechner durch Senden einer Aktualisierungsanforderung an den zweiten Rechner die Bildung eines neuen Paßwortes beim zweiten Rechner anfordern. Analog zuden obigen Ausführungen kann der zweite Rechner mit Hilfe einer  
20 bei ihm gespeicherten Kontrolldatenbank und dem entsprechenden Kontrollwert überprüfen, ob der erste Rechner seiner Anforderung zum Paßwortwechsel nachgekommen ist. Im negativen Fall kann der zweite Rechner die Kommunikation abbrechen und das Verfahren beenden.

In diesem Dokument sind folgende Veröffentlichungen zitiert:

- 5 [1] Microsoft Developer Network Library, Questions 151082  
S7D6D, S7590, S759E, S5970, Microsoft Press, Juli 1998,  
erhältlich am 29. September 1998 im Internet unter der  
folgenden Adresse:  
<http://msdn.microsoft.com/developer/>
- 10 [2] International Telecommunication Union, Draft ITU-T Recom-  
mendation H.235, Line Transmission of Non-Telephone Si-  
gnals, Security and Encryption for H Series (H.323 and  
Other H.245 Based) Multimedia Terminals), Version 1, Ka-  
pitel 10.3.2, September 1997
- 15 [3] International Telecommunication Union, Draft ITU-T Recom-  
mendation H.225.0, Line Transmission of Non-Telephone Si-  
gnals, Call Signaling Protocols and Media Stream Packe-  
tization for Packet Based Multimedia Communications Sy-  
stems, Version 2, Kapitel 7.6 und 7.16, March 1997
- 20 [4] International Telecommunication Union, X.680 - X.683: OSI  
NETWORKING AND SYSTEM ASPECTS - ABSTRACT SYNTAX NOTATION  
ONE (ASN.1), July 1994
- 25 [5] A. J. Menezes et al, Handbook of Applied Cryptography,  
CRC Press, New York, S. 497 - 504, 1997, ISBN 0-8493-  
8523-7

**Patentansprüche**

1. Verfahren zur Aktualisierung eines Paßwortes zwischen einem ersten Rechner und einem zweiten Rechner,
  - 5 a) bei dem der zweite Rechner im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht empfängt, wobei die Dienstanforderungsnachricht das Paßwort aufweist,
  - 10 b) bei dem mit der Dienstanforderungsnachricht von dem ersten Rechner die Erbringung eines Dienstes angefordert wird,
  - c) bei dem der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,
  - 15 d) bei dem für den Fall, daß das Paßwort gültig ist, der Dienst erbracht wird,
  - e) bei dem für den Fall, daß das Paßwort ungültig ist, von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet wird, mit der eine Aktualisierung
  - 20 des Paßworts gefordert wird, und
  - f) bei dem von dem ersten Rechner und/oder dem zweiten Rechner ein aktualisiertes Paßwort gebildet wird, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.
- 25 2. Verfahren nach Anspruch 1,  
bei dem die Bildung des aktualisierten Paßwortes auf folgende Weise erfolgt:
  - 30 a) der erste Rechner sendet eine Paßwortnachricht zu dem zweiten Rechner, in der das aktualisierte Paßwort enthalten ist in einer Weise, daß das aktualisierte Paßwort nur unter Verwendung des Paßwortes ermittelt werden kann,
  - b) der zweite Rechner ermittelt unter Verwendung des Paßwortes das aktualisierte Paßwort aus der Paßwortnachricht,
  - 35 c) der zweite Rechner speichert das aktualisierte Paßwort.
3. Verfahren nach Anspruch 2,

bei dem der zweite Rechner eine Bestätigungsnachricht sendet, mit der der Einsatz des aktualisierten Paßwortes im Rahmen der Kommunikationsverbindung bestätigt wird.

- 5    4. Verfahren nach einem der Ansprüche 1 bis 3,  
bei dem zu Beginn des Verfahrens der erste Rechner durch den zweiten Rechner authentifiziert wird unter Verwendung einer in der Dienstanforderungsnachricht enthaltenen Authentifikationsangabe des ersten Rechners.
- 10    5. Verfahren nach einem der Ansprüche 1 bis 4,  
bei dem die Überprüfung, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist, anhand einer Kontrolldatenbank erfolgt, in der für den  
15    ersten Rechner angegeben ist, ob zuvor schon von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet worden ist.
- 20    6. Verfahren nach einem der Ansprüche 1 bis 5,  
a) bei dem in der Dienstanforderungsnachricht eine Angabe enthalten zur Integritätssicherung der Dienstanforderungsnachricht,  
b) bei dem von dem zweiten Rechner die empfangene Dienstanforderungsnachricht auf ihre Integrität überprüft wird,  
25    c) bei dem nur für den Fall, daß die Integrität der Dienstanforderungsnachricht gewährleistet ist, das Verfahren durchgeführt wird, und  
d) sonst der angeforderte Dienst zurückgewiesen wird.
- 30    7. Verfahren nach einem der Ansprüche 2 bis 6,  
bei dem in der Paßwortnachricht das aktualisierte Paßwort verschlüsselt enthalten ist, wobei der Schlüssel zur Verschlüsselung des aktualisierten Paßwortes abhängig von dem Paßwort gebildet wird.
- 35    8. Verfahren nach Anspruch 7,

bei dem der Schlüssel durch mehrfache Aneinanderreihung des Paßwortes gebildet wird.

5 9. Anordnung mit mindestens einem ersten Rechner und mindestens einem zweiten Rechner zur Aktualisierung eines Paßwortes zwischen den Rechnern,

wobei der erste Rechner und der zweite Rechner jeweils einen Prozessor aufweisen, die derart eingerichtet sind, daß folgende Schritte durchführbar sind:

- 10 a) der zweite Rechner empfängt im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht, wobei die Dienstanforderungsnachricht das Paßwort aufweist,
- 15 b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,
- c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,
- 20 d) für den Fall, daß das Paßwort gültig ist, wird der Dienst erbracht,
- e) für den Fall, daß das Paßwort ungültig ist, wird von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet, mit der eine Aktualisierung des
- 25 Paßworts gefordert wird, und
- f) von dem ersten Rechner und/oder dem zweiten Rechner wird ein aktualisiertes Paßwort gebildet, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

30

10. Anordnung nach Anspruch 9,

bei der die Prozessoren derart eingerichtet sind, daß die Bildung des aktualisierten Paßwortes auf folgende Weise erfolgt:

- 35 a) der erste Rechner sendet eine Paßwortnachricht zu dem zweiten Rechner, in der das aktualisierte Paßwort enthal-

- ten ist in einer Weise, daß das aktualisierte Paßwort nur unter Verwendung des Paßwortes ermittelt werden kann,
- b) der zweite Rechner ermittelt unter Verwendung des Paßwortes das aktualisierte Paßwort aus der Paßwortnachricht,
- 5 c) der zweite Rechner speichert das aktualisierte Paßwort.

11. Anordnung nach Anspruch 9 oder 10,  
mit mehreren ersten Rechnern, die jeweils ein Paßwort gemeinsam mit dem zweiten Rechner besitzen, wobei das Paßwort jeweils eindeutig ist für die Kommunikationsverbindung zwischen  
10 dem jeweiligen ersten Rechner und dem zweiten Rechner.

12. Anordnung nach einem der Ansprüche 9 bis 11,  
mit mehreren zweiten Rechnern, die jeweils ein Paßwort gemeinsam mit jedem ersten Rechner besitzen, wobei das Paßwort jeweils eindeutig ist für die Kommunikationsverbindung zwischen dem jeweiligen zweiten Rechner und dem jeweiligen zweiten Rechner.  
15

**Zusammenfassung****Verfahren und Anordnung zur Aktualisierung eines Paßwortes**

- 5 Es erfolgt eine Aktualisierung eines Paßwortes zwischen einem  
ersten Rechner und einem zweiten Rechner, wobei
- a) der zweite Rechner im Rahmen einer zwischen dem ersten  
Rechner und dem zweiten Rechner bestehenden Kommunikati-  
onsverbindung eine von dem ersten Rechner gesendete
- 10 Dienstanforderungsnachricht empfängt, wobei die Dienstan-  
forderungsnachricht das Paßwort aufweist,
- b) mit der Dienstanforderungsnachricht wird von dem ersten  
Rechner die Erbringung eines Dienstes angefordert,
- c) der zweite Rechner überprüft, ob das in der Dienstanforde-  
15 rungsnachricht enthaltene Paßwort für den ersten Rechner  
gültig ist,
- d) für den Fall, daß das Paßwort gültig ist, der Dienst er-  
bracht wird,
- e) für den Fall, daß das Paßwort ungültig ist, von dem zwei-  
20 ten Rechner eine Aktualisierungsnachricht an den ersten  
Rechner gesendet wird, mit der eine Aktualisierung des  
Paßworts gefordert wird, und
- f) von dem ersten Rechner ein aktualisiertes Paßwort gebildet  
wird, welches im weiteren im Rahmen der Kommunikationsver-  
25 bindung als Paßwort verwendet wird.

FIG 1A

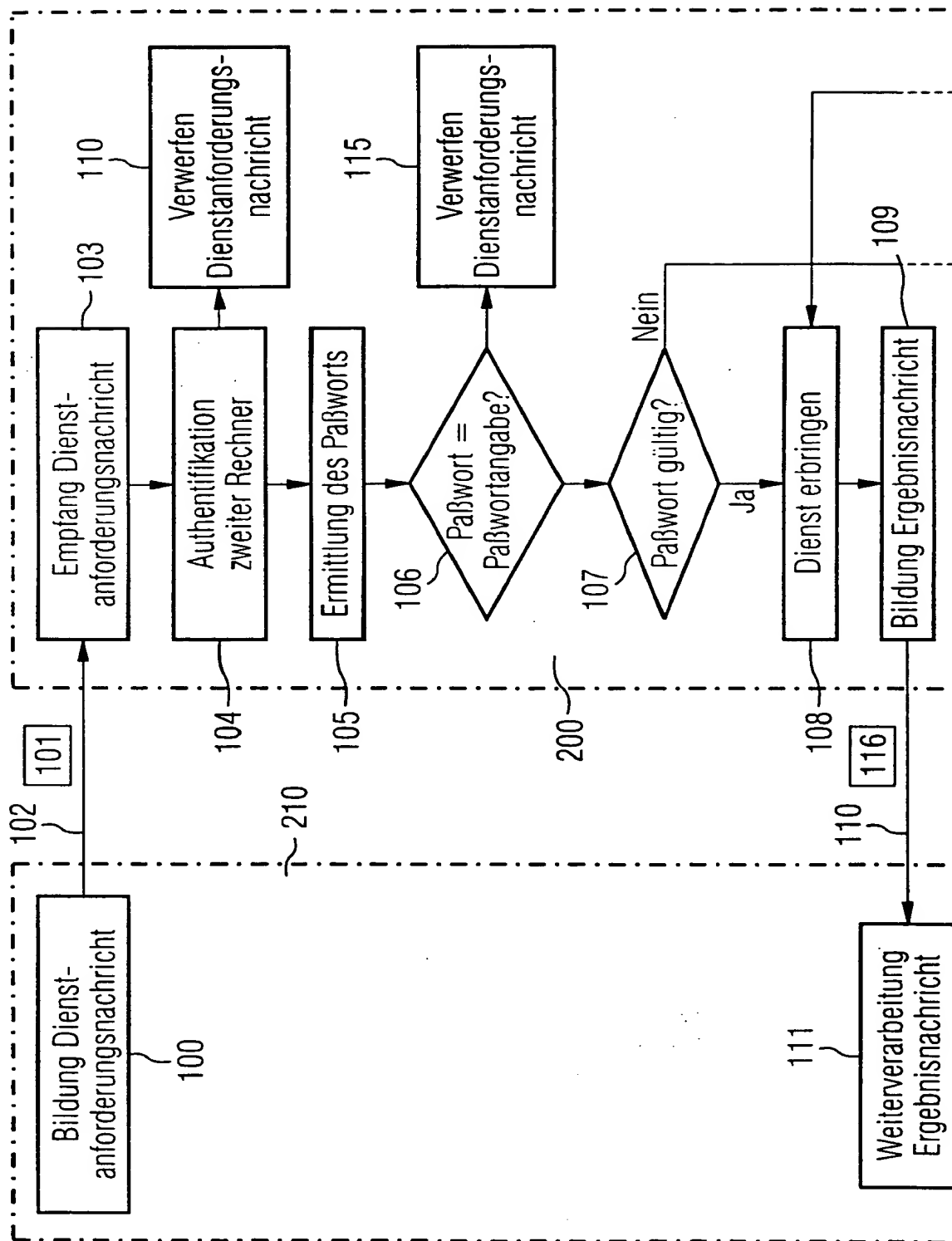




FIG 1B

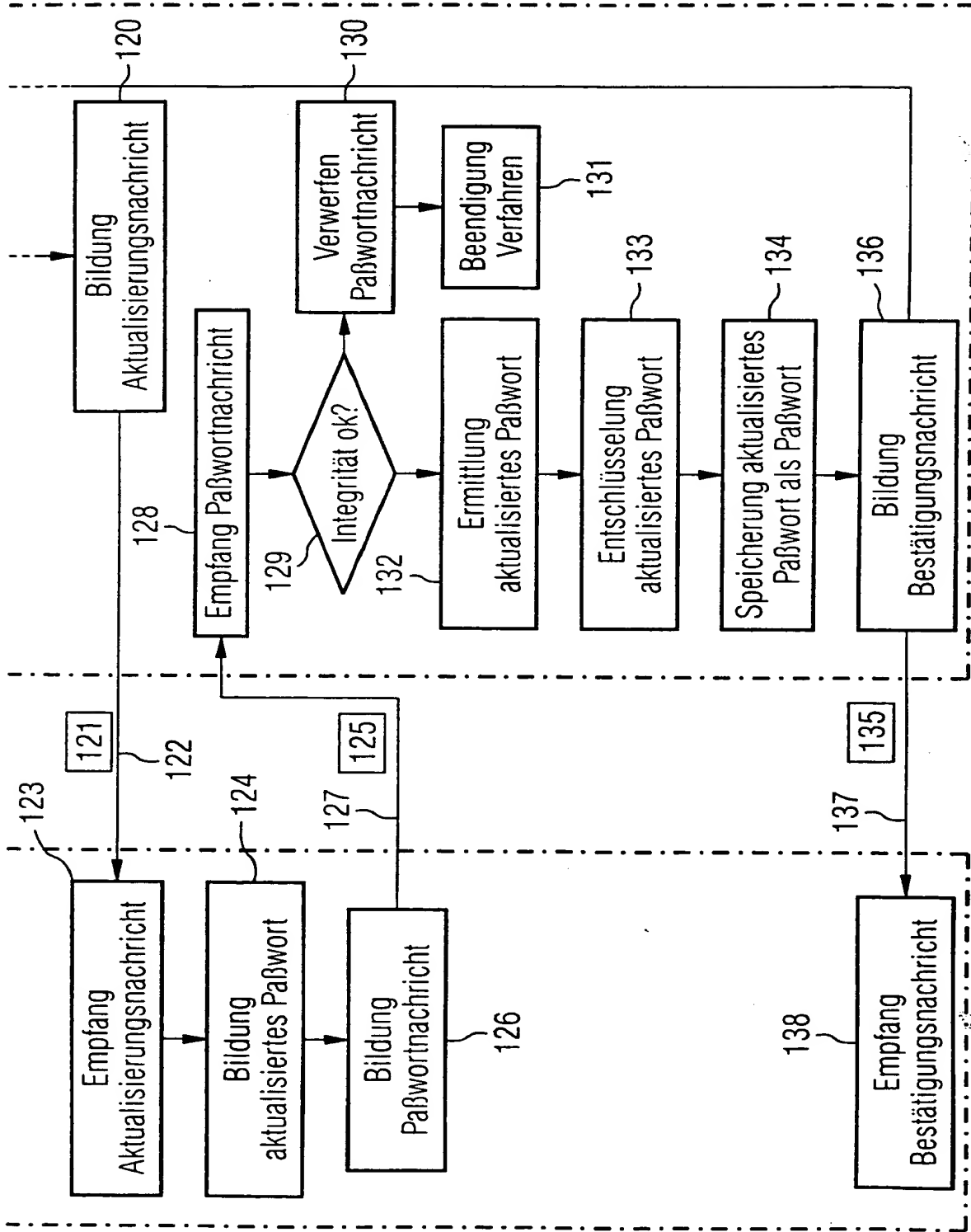
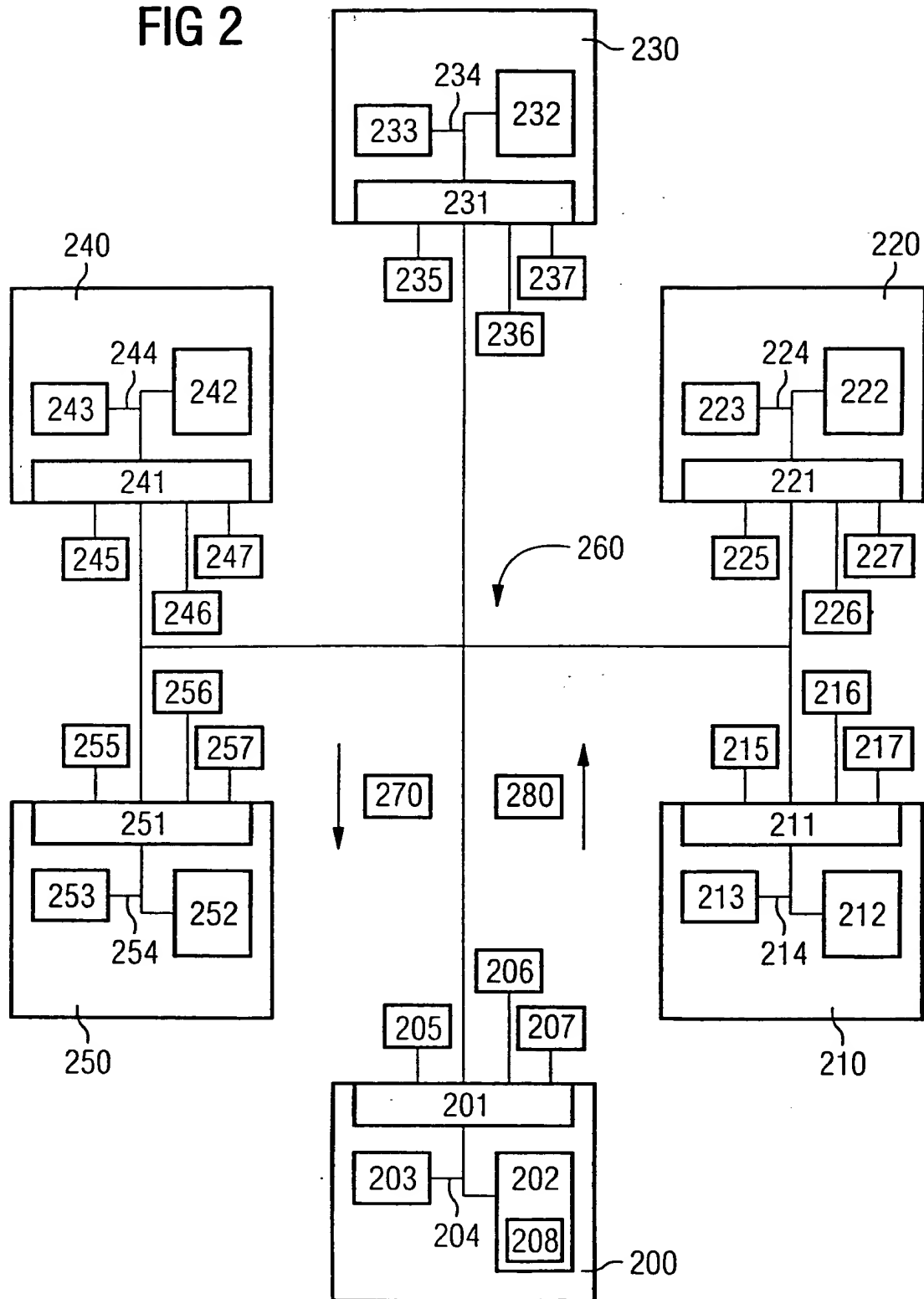


FIG 2



**Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens**  
**Patent Cooperation Treaty**  
**Traité de coopération en matière de brevets**

**PCT**

Anmeldenummer:

PCT/DE99/02844

23/11/2000

.....  
Datum (Tag / Monat / Jahr)



Harms, C

.....  
Bevollmächtigter Bediensteter der mit der  
internationalen vorläufigen Prüfung  
beauftragten Behörde

Beilage(n):

D1 = [http://www.devresource.hp.com/STK/man/11.00/passwd\\_1.html](http://www.devresource.hp.com/STK/man/11.00/passwd_1.html)

passwd(1)

passwd(1)

## NAME

passwd - change login password and associated attributes

## SYNOPSIS

passwd [name]

passwd -r files [-F file] [name]

passwd -r files [-e [shell]] [-gh] [name]

passwd -r files -s [-a]

passwd -r files -s [name]

passwd -r files [-d|-l] [-f] [-n min] [-w warn] [-x max] name

passwd -r nis [-e [shell]] [-gh] [name]

passwd -r nisplus [-e [shell]] [-gh] [-D domain] [name]

passwd -r nisplus -s [-a]

passwd -r nisplus -s [-D domain] [name]

passwd -r nisplus [-l] [-f] [-n min] [-w warn] [-x max] [-D domain]  
name

passwd -r dce [-e [shell]] [-gh] [name]

## DESCRIPTION

The passwd command modifies the password as well as the attributes associated with the login name. If name is omitted, it defaults to the invoking user's login name, which is determined using getlogin(3c).

The default password file is /etc/passwd. The -F option can be used to choose an alternate password file, where read and write permissions are required. This option is only available using the files repository.

Ordinary users can only change passwords corresponding to their login name. If an old password has been established, it is requested from the user. If valid, a new password is obtained. Once the new password is entered, it is determined if the old password has "aged" sufficiently. If password aging is not sufficient, the new password is rejected and passwd terminates (see passwd(4)).

If password aging and construction requirements are met, the password is re-entered to ensure consistency. If the new copy differs, passwd repeats the new password prompting cycle three times.

- 1 -

passwd(1)

passwd(1)

A superuser, whose effective user ID is zero (see id(1) and su(1)), is allowed to change any password and is not forced to comply with password aging. Superusers are not prompted for old passwords unless they are attempting to change the superuser's password in a trusted system. In addition, on untrusted systems, superusers are not forced to comply with password construction requirements. Null passwords can be created by entering a carriage return in response to the prompt for a new password.

The DCE repository (-r dce) is only available if Integrated Login has been configured, see *auth.adm(1m)*. If Integrated Login has been configured, other considerations apply. A user with appropriate DCE privileges is capable of modifying a user's password, shell, *gecos* or home directory - this is not dependent upon superuser privileges.

If the repository is not specified, i.e. *passwd [name]*, the password is changed in all existing repositories configured in */etc/nsswitch.conf*. If password options are used, and no repository is specified, the default repository is *files*.

#### Options

The following options are recognized:

- D *domain*      Use the *passwd.org\_dir* in the specified *domain*. This option is for *nisplus* repositories only. If not specified, the default *domain* is returned.
- e *shell*        Modify the default shell for the user's login name in the password file. If the *shell* is not provided, the user will be prompted to enter the default login shell.
- F *name*        Choose an alternative password file, where read and write permissions are required. This option is available for the *files* repository only.
- g                Change the *gecos* information in the password file, which is used by the *finger* command. The user is prompted for each subfield: name, location, work phone, and home phone.
- h                Modify the default home directory in the password file. Only superuser is allowed to exercise this option.
- r *repository*   Specify the repository to which the operation is to be applied. Supported repositories include *files*, *nis*, *nisplus*, and *dce*. If repository is not specified, the default is *files*.
- s *name*        Display password attributes associated with the specified *name*. Superuser privilege is required if the *files* repository is specified. For *nisplus*, there are

- 2 -

*passwd(1)*

*passwd(1)*

no restrictions.

- s [-a]        Display password attributes for all users in the password file. The -a option must be used in conjunction with the -s option when no *name* is specified. For *nisplus*, this will display entries in the NIS+ *passwd* table in the local domain. For *files*, this is restricted to superuser.

#### Privileged User Options

A superuser can modify password aging characteristics associated with the user name using the following options:

- d              Allow user to login without a password by deleting it.
- f              Force user to change password upon next login by

expiring the current password.

- l Lock user account.
- n *min* Determine the minimum number of days, *min*, that must transpire before the user can change the password.
- w *warn* Specify the number of days, *warn*, prior to the password expiring when the user will be notified that the password needs to be changed. This option is only enabled when the system has been converted to a trusted, secure system. Refer to the *Managing Systems and Workgroups* manual for how to convert your HP-UX to a trusted, secure system.
- x *max* Determine the maximum number of days, *max*, a password can remain unchanged. The user must enter another password after that number of days has transpired, known as the password expiration time.

The *min* and *max* arguments are each represented in units of days. These arguments will be rounded up to the nearest week on a nontrusted HP-UX system. If the system is then converted to a trusted system, the number of days will be based on those weeks. If only one of the two arguments is supplied, then, if the other one does not exist, it is set to zero.

#### Password Construction Requirements

Passwords must be constructed to meet the following requirements:

- o A password must have at least six characters. Only the first eight characters are significant in an untrusted system.
- o Characters must be from the 7-bit US-ASCII character set; letters from the English alphabet.

- 3 -

#### passwd(1)

#### passwd(1)

- o A password must contain at least two letters and at least one numeric or special character.
- o A password must differ from the user's login name and any reverse or circular shift of that login name. For comparison purposes, an uppercase letter and its corresponding lowercase equivalent are treated as identical.
- o A new password must differ from the old one by at least three characters (one character for non super user if changed by the super user in a trusted system). For comparison purposes, an uppercase letter and its corresponding lowercase equivalent are treated as identical.

If the above restrictions are met, the `/etc/nsswitch.conf` file specifies the repositories for which the password must be modified. The following configurations are supported:

- o `passwd: files`
- o `passwd: files nisplus`
- o `passwd: files nis`

- o passwd: compat (--> files nis)
- o passwd: compat (--> files nisplus)
- o passwd\_compat: nisplus

#### Smart Card Login

If the user account is configured to use a Smart Card, the user password is stored in the card. This password has characteristics identical to a normal password stored on the system.

The password is retrieved automatically from the Smart Card when a valid PIN is entered. Therefore, it is not necessary to know the password, only the PIN.

Since passwd can be used with a Smart Card account, the Smart Card must be inserted into the Smart Card reader. The user is prompted for a PIN instead of a password during authentication.

Enter PIN:

If the system retrieves a valid old password from the card, a new password is requested (twice). If the new password meets all requirements, the system automatically overwrites the old password stored on the card with the new password.

- 4 -

passwd(1)

passwd(1)

Therefore, the new dialog resembles:

Enter PIN:  
New password:  
Re-enter new password:

A Smart Card account can be shared among users. If one user modifies the password, other users must use the scsync command to write the new password onto their cards.

The scpin command is used to change the Smart Card PIN.

#### SECURITY FEATURES

This section applies only to trusted systems. It describes additional capabilities and restrictions.

When passwd is invoked on a trusted system, the existing password is requested (if one is present). This initiates the password solicitation dialog which depends upon the type of password generation that has been enabled on the account. There are four possible options for password generation:

Random syllables	A pronounceable password made up of meaningless syllables.
Random characters	An unpronounceable password made up of random characters from the character set.
Random letters	An unpronounceable password made up of random letters from the alphabet.
User-supplied	A user-supplied password, subject to length and triviality restrictions.

Passwords can be greater than eight characters. The system administrator can specify the password length guidelines for the system generated options (random syllables, random characters, and random letters). The actual maximum password length depends upon several parameters set by the system administrator in the authentication database. System warnings are displayed if password lengths are either too long or short.

The system requires a *minimum* time to elapse before a password can be changed. This prevents reuse of an old password within an undesirable period of time.

A password expires after a period of time known as the *expiration* time. System warnings are displayed as expiration time approaches.

- 5 -

passwd(1)

passwd(1)

A password dies after a time period known as the *password lifetime*. After the lifetime passes, the account is locked until it is re-enabled by a system administrator. Once unlocked, the user is forced to change the password before account use.

The system administrator can enable accounts without passwords. If a user account is allowed to function without a password, the user can choose a null password by typing a carriage-return when prompted for a new password.

#### Password History

The system administrator can enable the password history feature to discourage users from reusing previously used passwords. To enable the password history feature, the system administrator should create a file (or open the file if it already exists) named `security` under directory `/etc/default` and append to it one line content `PASSWORD_HISTORY_DEPTH=number`. The line contains three keywords, `PASSWORD_HISTORY_DEPTH`, `=`, and a decimal number which is the desired depth for the password history check. If the number is 2, the user's new password will be checked against two previously used passwords. One is the current password, and the other one is the password used before the current password. A configuration of password history depth of 2 prevents users from alternating between two passwords. The maximum password history depth supported is 10 and the minimum password history depth supported is 1. A depth configuration of more than 10 will be treated as 10, and a depth configuration of less than 1 will be treated as 1.

The password history depth configuration is on a system basis and is supported in trusted system for users in files repository only. This feature does not support the users in NIS or NISPLUS repositories. Once the feature is enabled, all the users on the system are subject to the same check. If the password history configuration file `/etc/default/security` does not exist, or if the file exists but the required line is missing, or if the line exists but any of the three required keywords is missing, the password history check feature is automatically disabled. When the feature is disabled, the password history check depth is set to 1 and a password change is subject to all of the other rules for a new password including a check with the current password.

#### EXTERNAL INFLUENCES

##### International Code Set Support

Characters from single-byte character code sets are supported in



passwords.

## EXAMPLES

Change the password expiration date of user to 42 days in the files repository:

- 6 -

passwd(1)

passwd(1)

```
passwd -r files -x 42 user
```

Modify the minimum time between password changes of user1 to 7 days in the nisplus repository:

```
passwd -r nisplus -n 7 user1
```

Force user2 to establish a new password on the next login which will expire in 70 days and prohibit the user from changing the password until 7 days have transpired:

```
passwd -r files -f -x 70 -n 7 user2
```

## DEPENDENCIES

### Pluggable Authentication Modules (PAM)

PAM is an Open Group standard for user authentication, password modification, and account validation. In particular, `pam_chauthtok()` is invoked to perform all functions related to `passwd`. This includes establishing and changing a password, using `passwd` options, and displaying error messages.

## WARNING

Avoid password characters which have special meaning to the tty driver, such as # (erase) and @ (kill). You may not be able to login with these characters.

## FILES

<code>/etc/passwd</code>	Standard password file used by HP-UX.
<code>/tcb/files/auth/*/*</code>	Protected password database used when system is converted to trusted system.

## SEE ALSO

`chfn(1)`, `id(1)`, `login(1)`, `su(1)`, `crypt(3c)`, `getlogin(3c)`, `passwd(4)`, `auth(5)`, `auth.adm(1m)`, `auth.dce(5)`.

*Managing Systems and Workgroups*

### Pluggable Authentication Modules (PAM)

`pam_chauthtok(3)`, `pam(3)`, `pam.conf(4)`, `pam_user.conf(4)`.

### HP-UX Smart Card Login

`scpin(1)`, `scsync(1)`.

## STANDARDS CONFORMANCE

`passwd`: SVID2, SVID3, XPG2

Hewlett-Packard Company

- 7 - HP-UX Release 11.00: February 1998

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT

### INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>98P2821P</b>	<b>WEITERES VORGEHEN</b>	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen <b>PCT/DE 99/ 02844</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>08/09/1999</b>	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) <b>30/09/1998</b>
Anmelder  <b>SIEMENS AKTIENGESELLSCHAFT et al.</b>		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

**1. Grundlage des Berichts**

a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

☐ in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. ☐ **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

**4. Hinsichtlich der Bezeichnung der Erfindung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

**5. Hinsichtlich der Zusammenfassung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

☐ wie vom Anmelder vorgeschlagen

☐ keine der Abb.

☒ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ weil diese Abbildung die Erfindung besser kennzeichnet.

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**

IPK 7 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 752 636 A (SUN MICROSYSTEM) 8. Januar 1997 (1997-01-08) Spalte 3, Zeile 11 - Spalte 4, Zeile 19 Spalte 6, Zeile 35 - Spalte 10, Zeile 37; Ansprüche; Abbildungen 3,5 ----	1-10
A	US 5 611 048 A (JACOBS ET AL.) 11. März 1997 (1997-03-11) Spalte 2, Zeile 1 - Zeile 33 Spalte 5, Zeile 65 - Spalte 11, Zeile 25; Anspruch 1; Abbildungen 5-8 -----	1-10



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

16. Februar 2000

Absendedatum des internationalen Recherchenberichts

24/02/2000

Name und Postanschrift der Internationalen Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Soler, J

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 99/02844

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 752636	A	08-01-1997	US 5734718 A JP 9231174 A	31-03-1998 05-09-1997
US 5611048	A	11-03-1997	NONE	



<b>(51) Internationale Patentklassifikation <sup>7</sup> :</b>  <b>G06F 1/00</b>	<b>A1</b>	<b>(11) Internationale Veröffentlichungsnummer:</b> WO 00/19297  <b>(43) Internationales Veröffentlichungsdatum:</b> 6. April 2000 (06.04.00)
<b>(21) Internationales Aktenzeichen:</b> PCT/DE99/02844  <b>(22) Internationales Anmeldedatum:</b> 8. September 1999 (08.09.99)  <b>(30) Prioritätsdaten:</b> 198 45 055.9      30. September 1998 (30.09.98)    DE  <b>(71) Anmelder (für alle Bestimmungsstaaten ausser US):</b> SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE).  <b>(72) Erfinder; und</b> <b>(75) Erfinder/Anmelder (nur für US):</b> FRIES, Steffen [DE/DE]; Wagenbauerstrasse 5, D-81677 München (DE). EUCHNER, Martin [DE/DE]; Lorenzstrasse 2, D-81737 München (DE).  <b>(74) Gemeinsamer Vertreter:</b> SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D-80506 München (DE).		<b>(81) Bestimmungsstaaten:</b> US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  <b>Veröffentlicht</b> <i>Mit internationalem Recherchenbericht.</i> <i>Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>

(54) Title: METHOD AND ARRAY FOR UPDATING A PASSWORD

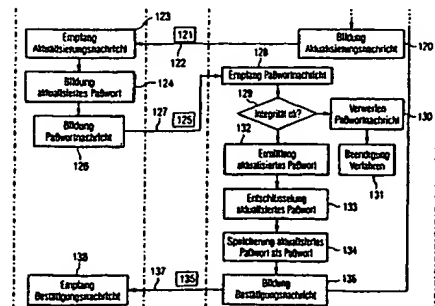
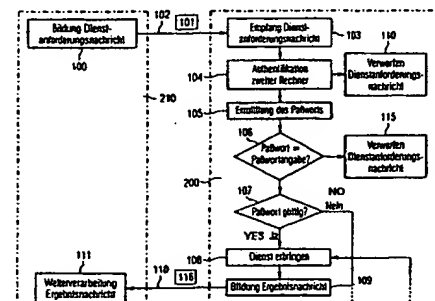
(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUR AKTUALISIERUNG EINES PASSWORTES

## (57) Abstract

Updating of a password is effected between a first and a second computer, wherein: (a) the second computer receives a service request message sent by the first computer during a communication link between the first and the second computers, wherein the service request message has a password; (b) the provision of a service is requested by the first computer in the service request message; (c) the second computer checks whether the password contained in the service request message is valid for the first computer; (d) the service is provided if the password is valid (e) if the password is not valid, the second computer sends an update message to the first computer requesting updating of the password and (f) an updated password is formed by the first computer which is used thereafter as password during communication link.

## (57) Zusammenfassung

Es erfolgt eine Aktualisierung eines Paßwortes zwischen einem ersten Rechner und einem zweiten Rechner, wobei (a) der zweite Rechner im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienst-anforderungsnachricht empfängt, wobei die Dienst-anforderungsnachricht das Paßwort aufweist; (b) mit der Dienst-anforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert; (c) der zweite Rechner überprüft, ob das in der Dienst-anforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist; (d) für den Fall, daß das Paßwort gültig ist, der Dienst erbracht wird; (e) für den Fall, daß das Paßwort ungültig ist, von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet wird, mit der eine Aktualisierung des Paßworts gefordert wird; und (f) von dem ersten Rechner ein aktualisiertes Paßwort gebildet wird, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.



100 ... FORMING SERVICE REQUEST MESSAGE  
 101 ... RECEPTION SERVICE REQUEST MESSAGE  
 104 ... AUTHENTICATION SECOND COMPUTER  
 105 ... DETERMINATION PASSWORD  
 106 ... PASSWORD = PASSWORD SPECIFICATION ?  
 107 ... PROVIDE SERVICE  
 109 ... FORMING RESULT MESSAGE  
 110, 115 ... REJECT SERVICE REQUEST MESSAGE  
 111 ... FURTHER PROCESS RESULT MESSAGE  
 120 ... RECEIVE UPDATE MESSAGE  
 124 ... FORMING UPDATED PASSWORD  
 126 ... FORMING PASSWORD MESSAGE  
 129 ... RECEIVE PASSWORD MESSAGE  
 130 ... INTEGRITY OK ?  
 131 ... REJECT PASSWORD MESSAGE  
 132 ... END PROCESS  
 133 ... DETERMINING UPDATES PASSWORD  
 134 ... ENCRYPTION UPDATES PASSWORD  
 135 ... STORAGE UPDATES PASSWORD AS PASSWORD  
 136 ... FORMING CONFIRMATION MESSAGE  
 137 ... RECEIVE CONFIRMATION MESSAGE

### LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

## Beschreibung

### Verfahren und Anordnung zur Aktualisierung eines Paßwortes

- 5 Die Erfindung betrifft ein Verfahren und eine Anordnung zur Aktualisierung eines Paßwortes.

Aus [1] sind ein solches Verfahren und eine solche Anordnung bekannt.

10

- Bei einer solchen Anordnung ist für den Fall, daß ein Benutzer diese Anordnung benutzen will, vorgesehen, daß von dem Benutzer eine Eingabe eines Paßwortes in die Anordnung gefordert wird. Nach Eingabe des Paßwortes durch den Benutzer wird  
15 von der Anordnung anhand einer Datenbank überprüft, ob eine eingegebene Paßwortangabe für den Benutzer ein gültiges Paßwort ist oder nicht.

- In der Datenbank der Anordnung ist eine Liste mit zulässigen Benutzern der Anordnung gespeichert. Jedem Benutzer ist jeweils ein Paßwort zugeordnet, welches gespeichert ist und mit dem das eingegebene Paßwort verglichen wird. Jedem Paßwort ist ferner eine Zeitangabe zugeordnet. Mit der Zeitangabe wird angegeben, für welchen Zeitraum das Paßwort gültig sein  
20 soll. Ist der Zeitraum abgelaufen, so wird das gespeicherte Paßwort ungültig und der Benutzer wird zu einer Aktualisierung des Paßwortes aufgefordert, wenn er die Benutzung der Anordnung aufnehmen will.

- 25 Auf diese Weise wird eine gewisse, von dem jeweiligen Zeitraum abhängige Aktualität des jeweiligen Paßwortes erreicht, wodurch ein höherer Sicherheitsgrad für die Anordnung hinsichtlich eines Mißbrauchs bzw. eines unbefugten Ermittels eines Paßworts gewährleistet wird. Ferner ist aus [1] bekannt, daß die Paßwortangabe in der Datenbank in kryptierter Form (verschlüsselt oder gebildet unter Verwendung einer Einweg-Hashfunktion) abgelegt werden kann. Aus [1] ist weiterhin  
35

bekannt, daß die Paßwortangabe kryptiert über eine Kommunikationsverbindung transportiert werden kann. Ein Beispiel dafür ist das Domain Logon bei Windows NT. Der Zeitpunkt des Paßwortwechsels ist jedoch auf den Zeitpunkt der Login-Prozedur  
5 beschränkt.

Aus [2] ist ein Kommunikationsstandard, der H.235-Standard, bekannt, in dem Rahmenbedingungen, insbesondere Formate von Nachrichten, die zwischen miteinander verbundenen Rechnern im  
10 Rahmen einer multimedialen Kommunikation ausgetauscht werden können.

Die Rechner können logisch oder fest miteinander verbunden sein.  
15

Ein Nachteil der aus [2] bekannten Verfahren ist insbesondere darin zu sehen, daß lediglich statische Paßworte für einen Benutzer eingesetzt werden können, wodurch die Wahrscheinlichkeit relativ hoch ist, daß in den Rechnern gespeicherte  
20 Paßworte irgendwann von einem unbefugten Dritten, einem Angreifer, ermittelt und mißbraucht werden können, wodurch die Sicherheit der einzelnen Rechner nicht mehr gewährleistet ist.

25 Aus [3] ist ein weiterer Kommunikationsstandard, der H.225-Standard, bekannt.

Aus [4] ist die sogenannte Abstract Syntax Notation 1 (ASN.1) beschrieben, die zur Definition des Formats einer Nachricht  
30 verwendet wird, die zur Definition des Formats einer Nachricht im Sinne der aus [2] und [3] bekannten Standards verwendet wird.

Eine Übersicht über Protokolle zur Aktualisierung kryptographischer Schlüssel ist in [5] zu finden.  
35



Insbesondere bei einem großen Kommunikationsnetz mit einer Vielzahl miteinander verbundenen Rechnern, beispielsweise dem Internet, stellt die oben beschriebene Situation ein hohes Risiko dar.

5

Somit liegt der Erfindung das Problem zugrunde, ein Verfahren und eine Anordnung zur Aktualisierung eines Paßwortes zwischen zwei miteinander verbundenen Rechnern anzugeben.

- 10 Das Problem wird durch die Anordnung sowie das Verfahren mit den Merkmalen gemäß den unabhängigen Ansprüchen gelöst.

Ein Verfahren zur Aktualisierung eines Paßwortes zwischen einem ersten Rechner und einem zweiten Rechner, weist folgende Schritte auf:

15

- a) der zweite Rechner empfängt im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht, wobei die Dienstanforderungsnachricht das Paßwort aufweist,
- 20 b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,
- c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,
- 25 d) für den Fall, daß das Paßwort gültig ist, wird der Dienst erbracht,
- e) für den Fall, daß das Paßwort ungültig ist, wird von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet, mit der eine Aktualisierung des Paßworts gefordert wird, und
- 30 f) von dem ersten Rechner und/oder dem zweiten Rechner wird ein aktualisiertes Paßwort gebildet, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

35

- Eine Anordnung weist mindestens einen ersten Rechner und mindestens einen zweiten Rechner auf zur Aktualisierung eines Paßwortes zwischen den Rechnern,  
wobei der erste Rechner und der zweite Rechner jeweils einen
- 5 Prozessor aufweisen, die derart eingerichtet sind, daß folgende Schritte durchführbar sind:
- a) der zweite Rechner empfängt im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete
  - 10 Dienstanforderungsnachricht, wobei die Dienstanforderungsnachricht das Paßwort aufweist,
  - b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,
  - c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner
  - 15 gültig ist,
  - d) für den Fall, daß das Paßwort gültig ist, wird der Dienst erbracht,
  - e) für den Fall, daß das Paßwort ungültig ist, wird von dem
  - 20 zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet, mit der eine Aktualisierung des Paßworts gefordert wird, und
  - f) von dem ersten Rechner und/oder dem zweiten Rechner wird
  - 25 ein aktualisiertes Paßwort gebildet, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

Durch die Erfindung wird eine Aktualisierung eines Paßwortes zwischen zwei Rechnern während einer zwischen den beiden

30 Rechnern bestehenden Kommunikationsverbindung möglich. Der zweite Rechner kann den ersten Rechner anschaulich dazu zwingen, daß der erste Rechner das Paßwort zu aktualisieren hat, wenn der erste Rechner einen Dienst von dem zweiten Rechner anfordert. Damit gewährleistet der zweite Rechner die Aktualität der Paßworte, wodurch die Sicherheit der Kommunikation

35 zwischen den Rechnern erhöht wird.

Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

- Die im weiteren beschriebenen Weiterbildungen gelten sowohl für das Verfahren als auch die Anordnung, wobei bei der Weiterbildung der Anordnung jeweils die Prozessoren der Rechner derart eingerichtet sind, daß die Weiterbildung realisierbar ist.
- 10 Die Bildung des aktualisierten Paßwortes erfolgt in einer Weiterbildung auf folgende Weise:
- a) der erste Rechner sendet eine Paßwortnachricht zu dem zweiten Rechner, in der das aktualisierte Paßwort enthalten ist in einer Weise, daß das aktualisierte Paßwort nur unter Verwendung des Paßwortes ermittelt werden kann,
  - 15 b) der zweite Rechner ermittelt unter Verwendung des Paßwortes das aktualisierte Paßwort aus der Paßwortnachricht,
  - c) der zweite Rechner speichert das aktualisierte Paßwort.
- 20 Der zweite Rechner kann eine Bestätigungsnachricht senden, mit der der Einsatz des aktualisierten Paßwortes im Rahmen der Kommunikationsverbindung bestätigt wird.
- Zu Beginn des Verfahrens wird vorzugsweise der erste Rechner durch den zweiten Rechner authentifiziert unter Verwendung einer in der Dienstanforderungsnachricht enthaltenen Authentifikationsangabe des ersten Rechners. Damit wird das Sicherheitsniveau der jeweiligen Kommunikationsverbindung erhöht.
- 25 Die Überprüfung, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist, erfolgt in einer weiteren Ausgestaltung anhand einer Kontrolldatenbank, in der für den ersten Rechner angegeben ist, ob zuvor schon von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet worden ist. Durch diese Vereinfachung wird das Verfahren schneller durchführbar, da eine
- 30
- 35

erhebliche Rechenzeiteinsparung im Rahmen der Überprüfung erreicht wird.

5 In der Dienstanforderungsnachricht ist bevorzugt eine Angabe  
enthalten zur Integritätssicherung der Dienstanforderungs-  
nachricht, mit welcher Angabe von dem zweiten Rechner die  
empfangene Dienstanforderungsnachricht auf ihre Integrität  
hin überprüft wird. Nur für den Fall, daß die Integrität der  
Dienstanforderungsnachricht gewährleistet ist, wird das Ver-  
10 fahren durchgeführt; sonst wird der angeforderte Dienst zu-  
rückgewiesen. Damit wird das Sicherheitsniveau der jeweiligen  
Kommunikationsverbindung weiter erhöht.

15 In der Paßwortnachricht ist das aktualisierte Paßwort bevor-  
zugt verschlüsselt enthalten, wobei der Schlüssel zur Ver-  
schlüsselung des aktualisierten Paßwortes abhängig von dem  
Paßwort gebildet wird. Durch diese Weiterbildung wird ein Zu-  
sammenhang zwischen dem „alten“ Paßwort und dem aktualisier-  
ten Paßwort geschaffen, womit nur der Besitzer des Paßwortes  
20 das aktualisierte Paßwort überhaupt ermitteln kann. Damit  
wird der Schutz des aktualisierten Paßwortes bei dessen Über-  
tragung verbessert.

25 Der Schlüssel wird bevorzugt durch mehrfache Aneinanderrei-  
hung des Paßwortes gebildet.

Es sind vorzugsweise mehrere erste Rechner vorgesehen, die  
jeweils ein Paßwort gemeinsam mit dem zweiten Rechner besit-  
zen, wobei das Paßwort jeweils eindeutig ist für die Kommuni-  
30 kationsverbindung zwischen dem jeweiligen ersten Rechner und  
dem zweiten Rechner. Damit ist die Erfindung sehr gut ein-  
setzbar in einem großen Kommunikationsnetz, in dem ein Ser-  
ver, der zweite Rechner, mehreren Clients, den ersten Rech-  
nern, Dienste über das Kommunikationsnetz anbietet.

35 Ferner können mehrere zweite Rechnern vorgesehen sein, die  
jeweils ein Paßwort gemeinsam mit jedem ersten Rechner besit-

zen, wobei das Paßwort jeweils eindeutig ist für die Kommunikationsverbindung zwischen dem jeweiligen zweiten Rechner und dem jeweiligen zweiten Rechner.

- 5 Ein Ausführungsbeispiel der Erfindung ist in den Figuren dargestellt und wird im weiteren näher erläutert:

Es zeigen

- 10 Figur 1 ein Ablaufdiagramm, in dem die Verfahrensschritte des Ausführungsbeispiels dargestellt sind;

- Figur 2 eine Skizze, in der Rechner dargestellt sind, die über ein Kommunikationsnetz miteinander verbunden  
15 sind.

- Fig.2 zeigt einen ersten Rechner 200 mit einem Speicher 202 und einem Prozessor 203, die jeweils über einen Bus 204 miteinander und mit einer Eingangs-/Ausgangsschnittstelle 201  
20 verbunden sind.

- Über die Eingangs-/Ausgangsschnittstelle 201 ist der erste Rechner 200 mit einem Bildschirm 205, einer Tastatur 206 sowie einer Computermouse 207 verbunden.

- 25 Ferner ist der erste Rechner 200 über ein Kommunikationsnetz 260, in dem Beispiel ein ISDN-Netz (Integrated Services Digital Network) mit weiteren Rechnern 210, 220, 230, 240 und 250 verbunden.

- 30 In dem ersten Rechner 200 ist eine Datenbank 208 gespeichert.

- Die weiteren Rechner 210, 220, 230, 240 und 250 weisen jeweils ebenfalls einen Prozessor 213, 223, 233, 243 und 253  
35 sowie jeweils einen Speicher 212, 222, 232, 242 und 252 auf. Jeweils der Prozessor 213, 223, 233, 243 und 253 und der Speicher 212, 222, 232, 242 und 252 sind über jeweils einen

Bus 214, 224, 234, 244 und 254 über eine Eingangs-  
/Ausgangsschnittstelle 211, 221, 231, 241 und 251 mit dem  
Kommunikationsnetz 260 verbunden. Ferner sind die weiteren  
Rechner 210, 220, 230, 240 und 250 jeweils mit einem Bild-  
5 schirm 215, 225, 235, 245 und 255 sowie einer Tastatur 216,  
226, 236, 246 und 256 sowie einer Computermouse 217, 227, 237,  
247 und 257 verbunden.

Zwischen den Rechnern 200, 210, 220, 230, 240 und 250 erfolgt  
10 die Kommunikation, d.h. ein gesicherter Austausch multimedia-  
ler Daten, gemäß dem H.235-Standard, wie in [2] beschrieben.

Der erste Rechner 200 ist als ein Server ausgestaltet und  
stellt den weiteren Rechnern 210, 220, 230, 240 und 250 ver-  
15 schiedene Dienste zur Verfügung.

Im weiteren wird angenommen, daß ein zweiter Rechner 210 ei-  
nen Dienst von dem ersten Rechner 200 in Anspruch nehmen  
will.

20

Zu Beginn des Verfahrens wird eine Kommunikationsverbindung  
zwischen dem zweiten Rechner 210 und dem ersten Rechner 200  
gemäß den in [2] und [3] beschriebenen Verfahren aufgebaut.  
Nach erfolgter Initialisierung der Kommunikationsverbindung  
25 besteht zwischen dem zweiten Rechner 210 und dem ersten Rech-  
ner 200 eine logische Verbindung, d.h. der Kommunikationsver-  
bindung ist ein logischer Kanal zugeordnet, der eindeutig  
identifizierbar ist. Über den logischen Kanal werden zwischen  
den Rechnern 200, 210, 220, 230, 240, 250 Nachrichten 270,  
30 280 ausgetauscht.

Ist die Kommunikationsverbindung aufgebaut, kann durch den  
zweiten Rechner 210 von dem ersten Rechner 200 ein Dienst in  
Anspruch genommen, in diesem Fall eine Datenbankabfrage von  
35 einer in dem ersten Rechner 200 gespeicherten Datenbank 208.

Im weiteren wird das Verfahren beschrieben, das durchgeführt wird, wenn der zweite Rechner 210 von dem ersten Rechner 200 Daten aus dessen Datenbank 208 ermitteln möchte.

- 5 Die gewünschten Kriterien für die Datenbankabfrage werden von einem Benutzer des zweiten Rechners 210 in den zweiten Rechner 210 eingegeben. Von dem zweiten Rechner 210 wird eine Dienstanforderungsnachricht 101 gebildet (Schritt 100), in der die Kriterien für die Datenbankabfrage enthalten sind  
10 (vgl. Fig.1).

Ferner sind in der Dienstanforderungsnachricht 101 folgende Größen enthalten:

- eine Authentifikationsangabe (Authentication Token), mit  
15 der eine Authentifikation des zweiten Rechners 210 durch den ersten Rechner 200 möglich ist; die Authentifikationsangabe erlaubt die Darstellung des Passwortes in verschiedener Form (beispielsweise verschlüsselt oder gebildet unter Verwendung einer Einweg-Hashfunktion als Einweg-Hashwert);
- 20 - eine H.235-Adresse, mit der der erste Rechner 200 eindeutig identifiziert wird;
- eine Passwortangabe PW des Benutzers des zweiten Rechners 210.

- 25 In dem ersten Rechner 200 ist für jeden weiteren Rechner 210, 220, 230, 240 und 250 ein dem jeweiligen Rechner 210, 220, 230, 240 und 250 zugeordnetes Passwort gespeichert. Ist in einer Dienstanforderungsnachricht 101, die von einem weiteren Rechner 210, 220, 230, 240 und 250 gebildet wird, eine Paß-  
30 wortangabe enthalten, die gleich dem gespeicherten Passwort für den weiteren Rechner 210, 220, 230, 240 und 250 ist, so wird der angeforderte Dienst dem Benutzer gewährt, d.h. von dem ersten Rechner 200 ausgeführt.

- 35 Dem Passwort ist jeweils eine erste Zeitangabe t1 zugeordnet, mit der angegeben wird, zu welchem Zeitpunkt das Passwort gebildet worden ist. Ferner ist dem Passwort jeweils eine zweite

10

Zeitangabe  $t_2$  zugeordnet, mit der angegeben wird, für welchen Zeitraum das Paßwort gültig ist.

Die Dienstanforderungsnachricht 101 wird von dem zweiten  
5 Rechner 210 an den ersten Rechner 200 übertragen  
(Schritt 102).

Nach Empfang der Dienstanforderungsnachricht 101 in dem ersten Rechner 200 (Schritt 103) wird der zweite Rechner 210  
10 unter Verwendung der Authentifikationsangabe in der Dienstanforderungsnachricht 101 authentifiziert (Schritt 104).

Nach positiver Authentifikation des zweiten Rechners 210 wird in einem weiteren Schritt (Schritt 105) die Paßwortangabe PW  
15 aus der Authentifikationsangabe der Dienstanforderungsnachricht 101 ermittelt und die Paßwortangabe wird mit dem in dem ersten Rechner 200 gespeicherten Paßwort, welches dem zweiten Rechner 200 zugeordnet ist, verglichen (Schritt 106).

20 Bei negativer Authentifikation wird die Dienstanforderungsnachricht 101 verworfen (Schritt 110) und der angeforderte Dienst wird nicht ausgeführt.

Stimmen die Paßwortangabe PW und das dem zweiten Rechner 200  
25 zugeordnete Paßwort überein, so wird überprüft, ob das Paßwort gültig ist (Schritt 107). Dies erfolgt in der Weise, daß eine aktuelle Zeit  $t_3$ , zu der die Dienstanforderungsnachricht 101 von dem ersten Rechner 200 empfangen worden ist, ermittelt wird.

30 Stimmen die Paßwortangabe PW und das dem zweiten Rechner 200 zugeordnete Paßwort überein, so wird die Dienstanforderungsnachricht 101 verworfen (Schritt 115) und der angeforderte Dienst wird nicht ausgeführt.

35



11

Es wird überprüft, ob die aktuelle Zeit  $t_3$  kleiner oder gleich ist der Summe aus der ersten Zeitangabe  $t_1$  und der zweiten Zeitangabe  $t_2$ , also ob gilt:

$$5 \quad t_3 \leq t_1 + t_2. \quad (1)$$

Ist Vorschrift (1) erfüllt, so bedeutet dies, daß die Paßwortangabe dem Paßwort entspricht und das Paßwort noch gültig ist.

10

In diesem Fall wird der mit der Dienstanforderung 101 angeforderte Dienst, also die Datenbankabfrage von dem ersten Rechner 200 durchgeführt (Schritt 108) und das Ergebnis der Datenbankabfrage wird in einer gebildeten Ergebnismeldung  
15 116 (Schritt 109) an den zweiten Rechner 210 übertragen (Schritt 110), in dem das Ergebnis der Datenbankabfrage weiterverarbeitet wird (Schritt 111).

Ist Vorschrift (1) nicht erfüllt, so bedeutet dies, daß zwar  
20 der zweite Rechner 210 aufgrund der erfolgten Authentifikation grundsätzlich zur Anforderung des Dienstes berechtigt ist, das dem zweiten Rechner 210 zugeordnete Paßwort nicht mehr gültig ist.

25 In einem weiteren Schritt (Schritt 120) wird bei ungültigem Paßwort von dem ersten Rechner 200 eine Aktualisierungsmeldung 121 gebildet und an den zweiten Rechner 210 gesendet (Schritt 122), mit der eine Aktualisierung des Paßworts gefordert wird. Ferner wird von dem ersten Rechner 200 in einer  
30 Kontrolldatenbank ein Bit (Kontrollwert) auf einen ersten Wert gesetzt, mit dem angegeben wird, daß das jeweilige Paßwort ungültig ist und die entsprechende Aktualisierungsmeldung 121 an den zweiten Rechner 210 gesendet worden ist.

35 Nach Empfang der Aktualisierungsmeldung 121 (Schritt 123) wird von dem zweiten Rechner ein aktualisiertes Paßwort  $aPW$  gebildet (Schritt 124).

- Hält sich der zweite Rechner 210 nicht an die vorgeschriebene Prozedur und generiert erneut eine Dienstanforderung, ohne das Paßwort zu ändern, so kann der erste Rechner 200 dies
- 5 nach der Authentifikation des zweiten Rechners 210 und dem Überprüfen des Kontrollwertes feststellen. Ist der Kontrollwert auf den ersten Wert gesetzt, so kann das Verfahren beendet werden (Schritt 131).
- 10 Das aktualisierte Paßwort aPW wird symmetrisch gemäß dem Data Encryption Standard (DES) verschlüsselt. Als Schlüssel wird das Paßwort PW, welches auch in dem zweiten Rechner 210 bekannt und gespeichert ist, zur Verschlüsselung des aktualisierten Paßworts aPW verwendet.
- 15 Das verschlüsselte aktualisierte Paßwort aPW wird in einer von dem zweiten Rechner 210 gebildeten Paßwortnachricht 125 (Schritt 126) an den ersten Rechner übertragen (Schritt 127).
- 20 In der Paßwortnachricht 125 ist eine Integritätsangabe enthalten, mit der die Integrität der Paßwortnachricht 125 überprüft werden kann.
- Nach Empfang der Paßwortnachricht 125 (Schritt 128) wird die
- 25 Integrität der Paßwortnachricht 125 überprüft (Schritt 129).
- Bei negativer Integritätsprüfung wird die Paßwortnachricht 125 verworfen (Schritt 130) und das Verfahren beendet (Schritt 131).
- 30 Bei positiver Integritätsprüfung wird von dem ersten Rechner 200 das verschlüsselte aktualisierte Paßwort aPW ermittelt (Schritt 132) und das aktualisierte Paßwort aPW wird entschlüsselt (Schritt 133).
- 35 Das ermittelte aktualisierte Paßwort aPW wird in einem weiteren Schritt als neues Paßwort für den zweiten Rechner 210 ge-

13

speichert (Schritt 134). Ferner wird von dem ersten Rechner 200 in der Kontrolldatenbank der entsprechende Kontrollwert auf einen zweiten Wert gesetzt, mit dem angegeben wird, daß das jeweilige Paßwort gültig ist.

5

Anschließend wird von dem ersten Rechner 200 eine Bestätigungsnachricht 135 gebildet (Schritt 136) und an den zweiten Rechner 210 übertragen (Schritt 137) und von dem zweiten Rechner 210 empfangen (Schritt 138). Mit der Bestätigungsnachricht 135 wird dem zweiten Rechner 210 der weitere Einsatz des aktualisierten Paßwortes aPW im Rahmen der Kommunikationsverbindung bestätigt.

Weiterhin wird von dem ersten Rechner 200 der Dienst erbracht (Schritt 108), die Ergebnismnachricht 116 gebildet (Schritt 109) und die Ergebnismnachricht 116 an den zweiten Rechner 210 übertragen (Schritt 110). In dem zweiten Rechner 210 wird die Ergebnismnachricht 116 weiterverarbeitet (Schritt 111).

20

Ferner wird von dem ersten Rechner 200 in der Kontrolldatenbank das entsprechende Bit auf einen zweiten Wert gesetzt, mit dem angegeben wird, daß das jeweilige Paßwort gültig ist.

Bei einer weiteren empfangenen Dienstanforderungsnachricht wird jeweils nach deren Empfang von dem ersten Rechner 200 anhand der Kontrolldatenbank überprüft, ob das jeweilige Paßwort gültig ist oder nicht. Auf diese Weise wird eine sehr schnelle Prüfung des Paßwortes erreicht.

30

Die im Rahmen dieses Verfahrens verwendeten Nachrichten sind gemäß dem H.225.0-Standard, wie er in [3] beschrieben ist, codiert.

Zur Definition des im weiteren beschriebenen Formats der einzelnen Nachrichten wird die in [4] beschriebene Abstract Syntax Notation 1 (ASN.1) verwendet.

Die Nachrichten werden als eine in [3] vorgesehene NonStandardMessage codiert, wie im folgenden beschrieben:

```

5 NonStandardMessage ::= SEQUENCE
  {
    requestSeqNum      RequestSeqNum,
    nonStandardData    NonStandardParameter,
    ...
10    tokens            SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens       SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue ICV OPTIONAL
  }

15 NonStandardParameter ::= SEQUENCE
  {
    nonStandardIdentifier NonStandardIdentifier,
    data                  OCTET STRING
20  }

NonStandardIdentifier ::= CHOICE
  {
25    object            OBJECT IDENTIFIER,
    h221NonStandard    H221NonStandard,
    ...
  }

30 data ::= SEQUENCE
  {
    alias              GatekeeperIdentifier,
    confirm            boolean,
35    -- optionally for the provision of integrity
    rejectReason       PWUpdateRejectReason OPTIONAL,
    hash_algorithm     NonIsoIntegrityMechanism OPTIONAL,
    token              HASHED OPTIONAL,
40    -- < alias, confirmation, new password>
    ...
  }

45 PWUpdateRejectReason ::= CHOICE
  {
    notregistered      NULL, -- keep the old password
    pw_wrong           NULL, -- keep the old password
    pw_old             NULL, -- keep the old password
50    ...
  }

```

15

```

NonIsoIntegrityMechanism ::= CHOICE
{
  -- HMAC mechanism used, no truncation, tagging may bei dem
  necessary!
  HMAC-MD5          NULL,
5    HMAC-isol0118-2-s EncryptIntAlg,
    -- according to ISO/IEC 10118-2 using
    -- EncryptIntAlg as core block encryption algorithm
    -- (short MAC)
10   HMAC-isol0118-2-1 EncryptIntAlg,
    -- according to ISO/IEC 10118-2 using
    -- EncryptIntAlg as core block encryption algorithm
    -- (long MAC)
    HMAC-isol0118-3  OBJECT IDENTIFIER,
15   -- according to ISO/IEC 10118-3 using
    -- OID as hash function (OID is SHA-1, RIPE-MD160,
    -- RIPE-MD128)
    ...
}

20 EncryptIntAlg ::= CHOICE
{
  -- core encryption algorithms for RAS message integrity
  nonStandard      NonStandardParameter,
25  isoAlgorithm    OBJECT IDENTIFIER,      -- defined in
  ISO/IEC 9979
  ...
}

30 AliasAddress ::= CHOICE
{
  e164             IA5String (SIZE (1..128)) (FROM („0123456789#*,“)),
  h323-ID          BMPString (SIZE (1..256)),
35  ...
  url-ID           IA5String (SIZE (1..512)),
    -- URL style address
  transportID      TransportAddress,
  email-ID         IA5String (SIZE (1..512)),
40  ...
    -- rfc822-compliant email address
  partyNumber      PartyNumber
}

```

Im weiteren sind einige Alternativen zu dem oben beschriebenen  
 45 Ausführungsbeispiel dargestellt:

Die Art der Integritätssicherung ist grundsätzlich beliebig,  
 ebenso wie der Verschlüsselungsalgorithmus zur Verschlüsse-  
 lung des aktualisierten Paßwortes.

50

Die Realisierung der Nachrichten als Non Standard Messages  
 bzw. Non Standard Data Field ist nicht zwingend notwendig.  
 Die Darstellung der Nachrichten läßt sich auch über neu zu

definierende Nachrichten oder Protokollfelder in den aus [2] und [3] bekannten Standards realisieren.

5 Auch sind das Verfahren und die Anordnung nicht auf die aus [2] und [3] bekannten Standards beschränkt.

Die Bildung der Dienstanforderungsnachricht und/oder der Aktualisierungsnachricht und/oder der Paßwortnachricht und/oder der Bestätigungsnachricht können separat als eigenständige  
10 Nachrichten erfolgen und zwischen den beteiligten Rechnern separat übertragen werden. Es ist ferner in einer Variante möglich, die jeweilige Nachricht gemäß dem Prinzip des sogenannten "Piggybacks" gemeinsam mit anderen Nachrichten zwischen den beteiligten Rechnern zu übertragen.

15

Auch kann der zweite Rechner durch Senden einer Aktualisierungsanforderung an den zweiten Rechner die Bildung eines neuen Paßwortes beim zweiten Rechner anfordern. Analog zuden obigen Ausführungen kann der zweite Rechner mit Hilfe einer  
20 bei ihm gespeicherten Kontrolldatenbank und dem entsprechenden Kontrollwert überprüfen, ob der erste Rechner seiner Anforderung zum Paßwortwechsel nachgekommen ist. Im negativen Fall kann der zweite Rechner die Kommunikation abbrechen und das Verfahren beenden.

In diesem Dokument sind folgende Veröffentlichungen zitiert:

- [1] Microsoft Developer Network Library, Questions 151082 S7D6D, S7590, S759E, S5970, Microsoft Press, Juli 1998, erhältlich am 29. September 1998 im Internet unter der folgenden Adresse:  
<http://msdn.microsoft.com/developer/>
- [2] International Telecommunication Union, Draft ITU-T Recommendation H.235, Line Transmission of Non-Telephone Signals, Security and Encryption for H Series (H.323 and Other H.245 Based) Multimedia Terminals), Version 1, Kapitel 10.3.2, September 1997
- [3] International Telecommunication Union, Draft ITU-T Recommendation H.225.0, Line Transmission of Non-Telephone Signals, Call Signaling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems, Version 2, Kapitel 7.6 und 7.16, March 1997
- [4] International Telecommunication Union, X.680 - X.683: OSI NETWORKING AND SYSTEM ASPECTS - ABSTRACT SYNTAX NOTATION ONE (ASN.1), July 1994
- [5] A. J. Menezes et al, Handbook of Applied Cryptography, CRC Press, New York, S. 497 - 504, 1997, ISBN 0-8493-8523-7

**Patentansprüche**

1. Verfahren zur Aktualisierung eines Paßwortes zwischen einem ersten Rechner und einem zweiten Rechner,
  - 5 a) bei dem der zweite Rechner im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht empfängt, wobei die Dienstanforderungsnachricht das Paßwort aufweist,
  - 10 b) bei dem mit der Dienstanforderungsnachricht von dem ersten Rechner die Erbringung eines Dienstes angefordert wird,
  - c) bei dem der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,
  - 15 d) bei dem für den Fall, daß das Paßwort gültig ist, der Dienst erbracht wird,
  - e) bei dem für den Fall, daß das Paßwort ungültig ist, von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet wird, mit der eine Aktualisierung
  - 20 des Paßworts gefordert wird, und
  - f) bei dem von dem ersten Rechner und/oder dem zweiten Rechner ein aktualisiertes Paßwort gebildet wird, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.
- 25 2. Verfahren nach Anspruch 1,  
bei dem die Bildung des aktualisierten Paßwortes auf folgende Weise erfolgt:
  - a) der erste Rechner sendet eine Paßwortnachricht zu dem
  - 30 zweiten Rechner, in der das aktualisierte Paßwort enthalten ist in einer Weise, daß das aktualisierte Paßwort nur unter Verwendung des Paßwortes ermittelt werden kann,
  - b) der zweite Rechner ermittelt unter Verwendung des Paßwortes das aktualisierte Paßwort aus der Paßwortnachricht,
  - 35 c) der zweite Rechner speichert das aktualisierte Paßwort.
3. Verfahren nach Anspruch 2,



bei dem der zweite Rechner eine Bestätigungsnachricht sendet, mit der der Einsatz des aktualisierten Paßwortes im Rahmen der Kommunikationsverbindung bestätigt wird.

- 5    4. Verfahren nach einem der Ansprüche 1 bis 3,  
bei dem zu Beginn des Verfahrens der erste Rechner durch den zweiten Rechner authentifiziert wird unter Verwendung einer in der Dienstanforderungsnachricht enthaltenen Authentifikationsangabe des ersten Rechners.
- 10
5. Verfahren nach einem der Ansprüche 1 bis 4,  
bei dem die Überprüfung, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist, anhand einer Kontrolldatenbank erfolgt, in der für den  
15    ersten Rechner angegeben ist, ob zuvor schon von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet worden ist.
6. Verfahren nach einem der Ansprüche 1 bis 5,
- 20    a) bei dem in der Dienstanforderungsnachricht eine Angabe enthalten zur Integritätssicherung der Dienstanforderungsnachricht,  
b) bei dem von dem zweiten Rechner die empfangene Dienstanforderungsnachricht auf ihre Integrität überprüft wird,  
25    c) bei dem nur für den Fall, daß die Integrität der Dienstanforderungsnachricht gewährleistet ist, das Verfahren durchgeführt wird, und  
d) sonst der angeforderte Dienst zurückgewiesen wird.
- 30    7. Verfahren nach einem der Ansprüche 2 bis 6,  
bei dem in der Paßwortnachricht das aktualisierte Paßwort verschlüsselt enthalten ist, wobei der Schlüssel zur Verschlüsselung des aktualisierten Paßwortes abhängig von dem Paßwort gebildet wird.
- 35
8. Verfahren nach Anspruch 7,

bei dem der Schlüssel durch mehrfache Aneinanderreihung des Paßwortes gebildet wird.

9. Anordnung mit mindestens einem ersten Rechner und mindestens einem zweiten Rechner zur Aktualisierung eines Paßwortes zwischen den Rechnern,  
wobei der erste Rechner und der zweite Rechner jeweils einen Prozessor aufweisen, die derart eingerichtet sind, daß folgende Schritte durchführbar sind:
- 10 a) der zweite Rechner empfängt im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht, wobei die Dienstanforderungsnachricht das Paßwort aufweist,
  - 15 b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,
  - c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,
  - 20 d) für den Fall, daß das Paßwort gültig ist, wird der Dienst erbracht,
  - e) für den Fall, daß das Paßwort ungültig ist, wird von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet, mit der eine Aktualisierung des
  - 25 Paßworts gefordert wird, und
  - f) von dem ersten Rechner und/oder dem zweiten Rechner wird ein aktualisiertes Paßwort gebildet, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.
- 30 10. Anordnung nach Anspruch 9,  
bei der die Prozessoren derart eingerichtet sind, daß die Bildung des aktualisierten Paßwortes auf folgende Weise erfolgt:
- 35 a) der erste Rechner sendet eine Paßwortnachricht zu dem zweiten Rechner, in der das aktualisierte Paßwort enthal-

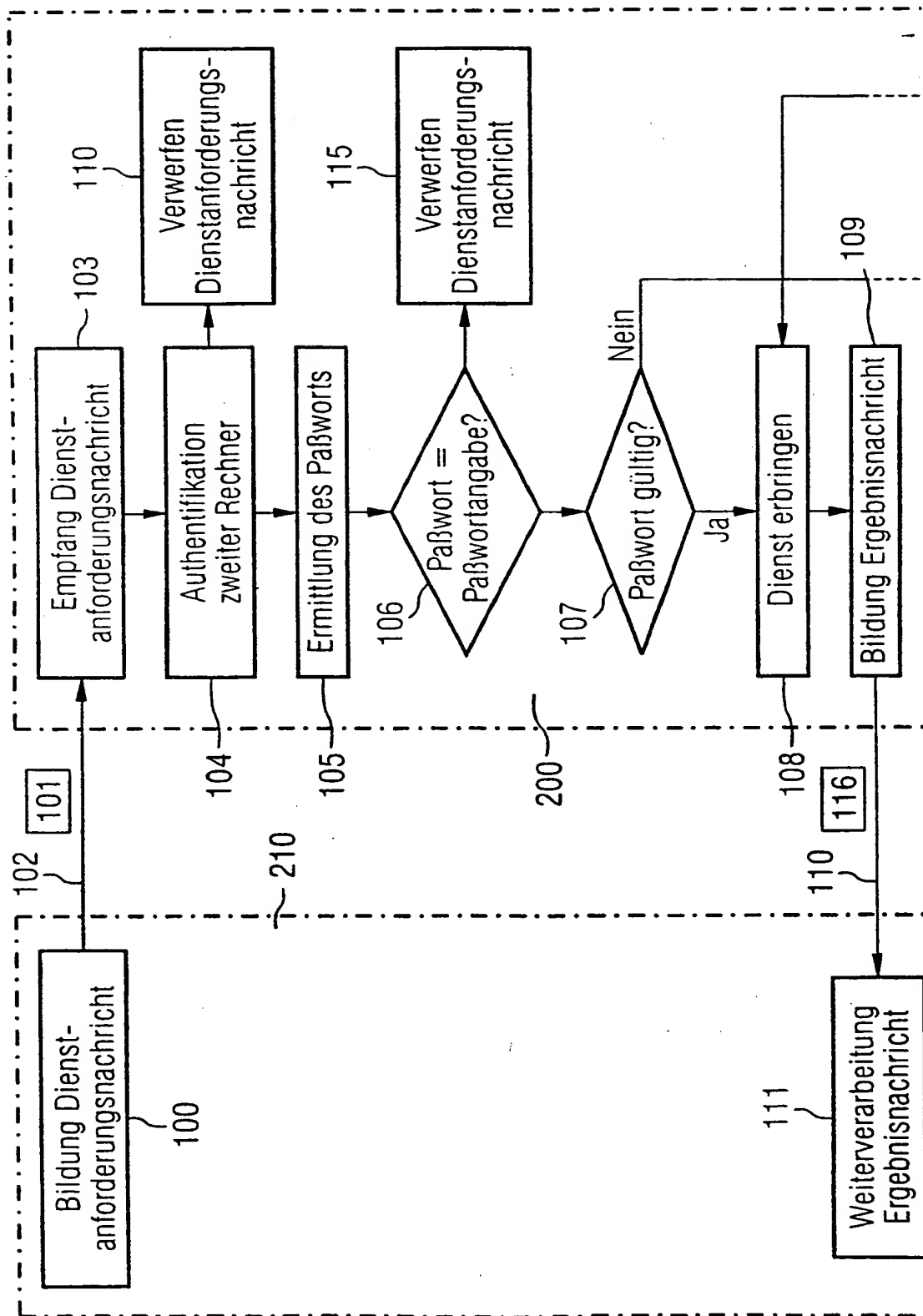
- ten ist in einer Weise, daß das aktualisierte Paßwort nur unter Verwendung des Paßwortes ermittelt werden kann,
- b) der zweite Rechner ermittelt unter Verwendung des Paßwortes das aktualisierte Paßwort aus der Paßwortnachricht,
- 5 c) der zweite Rechner speichert das aktualisierte Paßwort.

11. Anordnung nach Anspruch 9 oder 10,  
mit mehreren ersten Rechnern, die jeweils ein Paßwort gemeinsam mit dem zweiten Rechner besitzen, wobei das Paßwort je-  
10 weils eindeutig ist für die Kommunikationsverbindung zwischen dem jeweiligen ersten Rechner und dem zweiten Rechner.

12. Anordnung nach einem der Ansprüche 9 bis 11,  
mit mehreren zweiten Rechnern, die jeweils ein Paßwort ge-  
15 meinsam mit jedem ersten Rechner besitzen, wobei das Paßwort jeweils eindeutig ist für die Kommunikationsverbindung zwischen dem jeweiligen zweiten Rechner und dem jeweiligen zweiten Rechner.

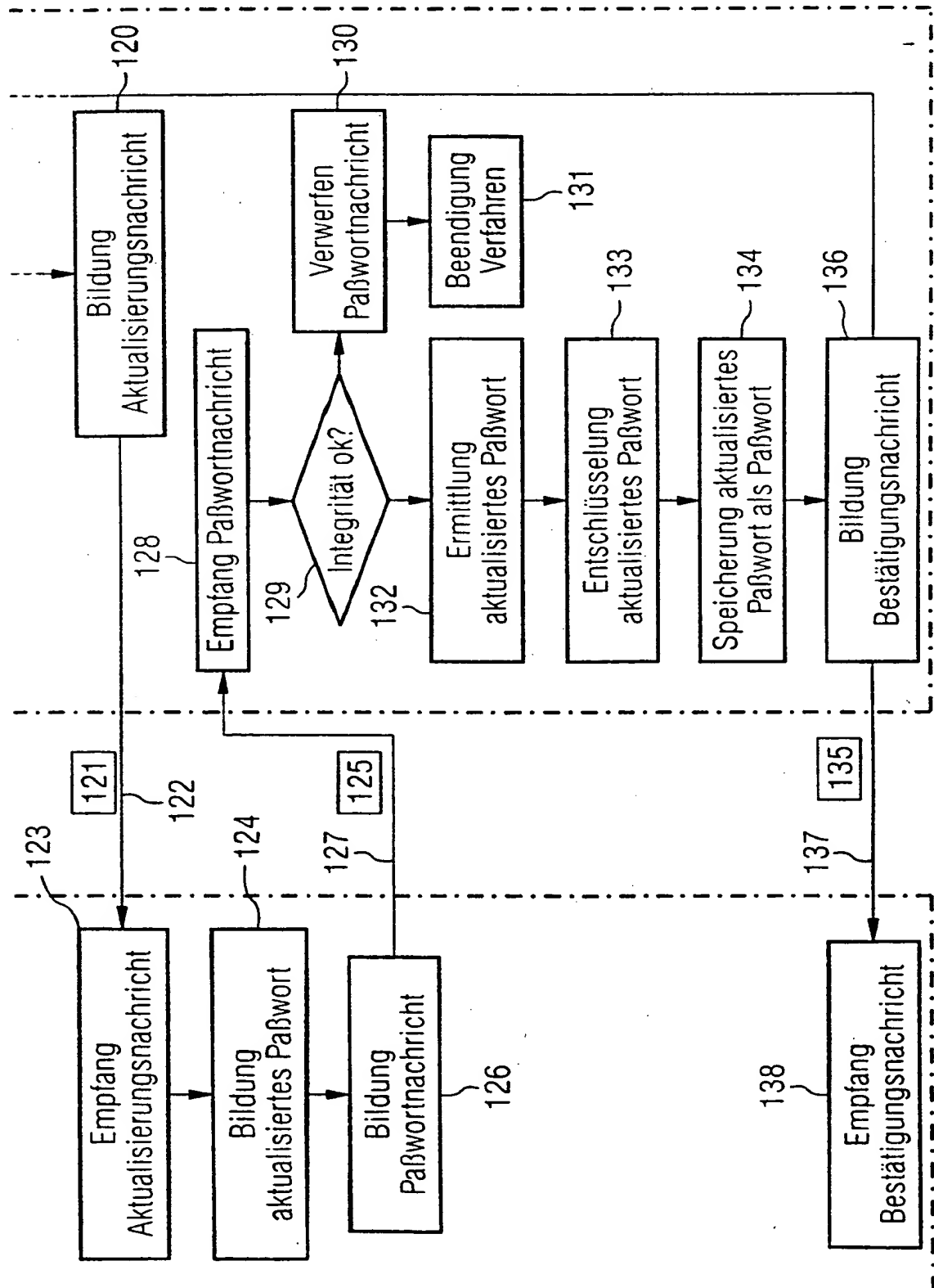
1/3

FIG 1A



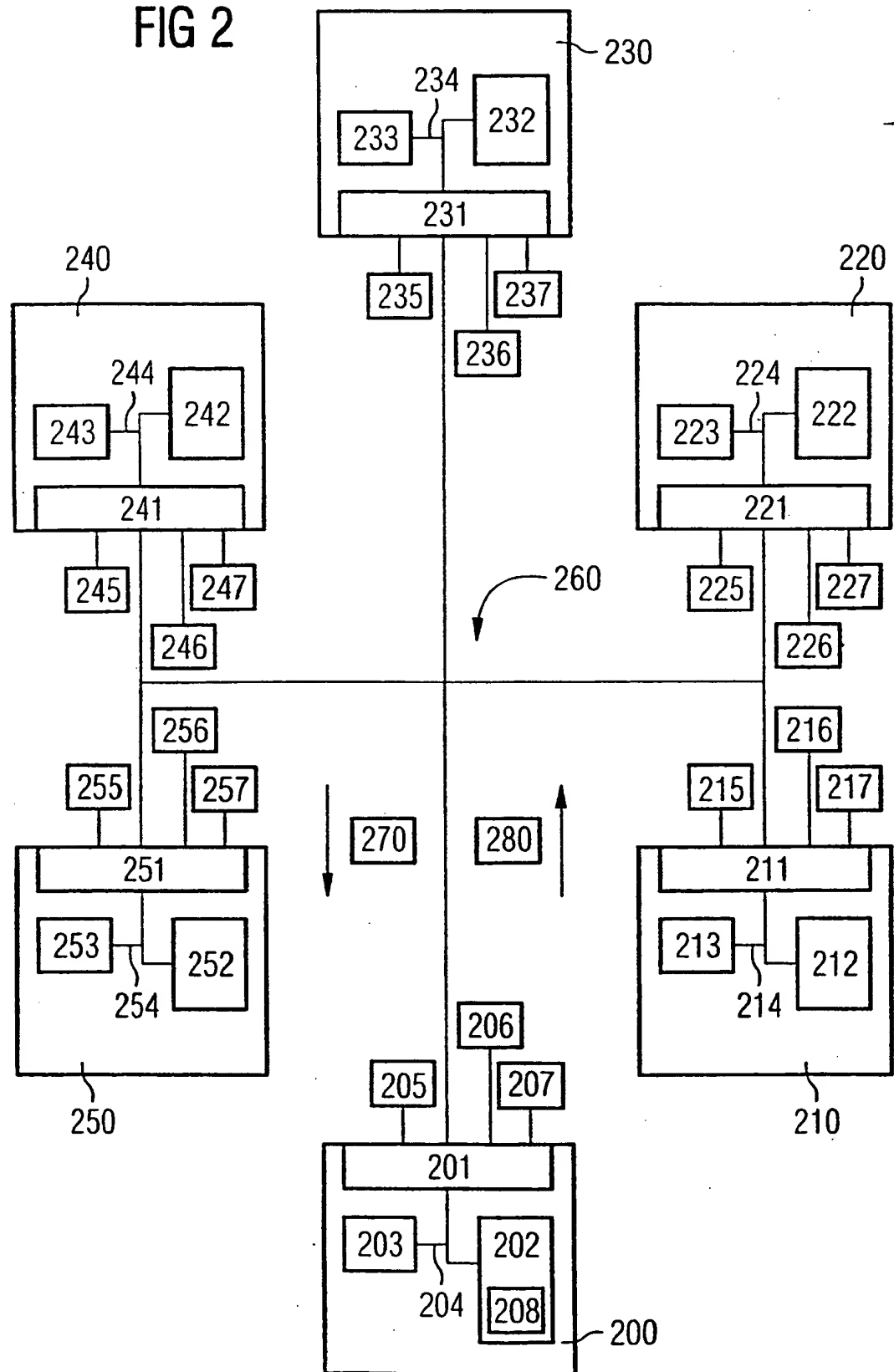
2/3

FIG 1B



3/3

FIG 2



## INTERNATIONAL SEARCH REPORT

International Application No.

PCT/DE 99/02844

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 752 636 A (SUN MICROSYSTEM) 8 January 1997 (1997-01-08) column 3, line 11 -column 4, line 19 column 6, line 35 -column 10, line 37; claims; figures 3,5	1-10
A	US 5 611 048 A (JACOBS ET AL.) 11 March 1997 (1997-03-11) column 2, line 1 - line 33 column 5, line 65 -column 11, line 25; claim 1; figures 5-8	1-10



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

## \* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"A" document member of the same patent family

Date of the actual completion of the international search

16 February 2000

Date of mailing of the international search report

24/02/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3018

Authorized officer

Soler, J

## INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/DE 99/02844

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 752636	A	08-01-1997	US 5734718 A JP 9231174 A	31-03-1998 05-09-1997
US 5611048	A	11-03-1997	NONE	



# INTERNATIONALER RECHERCHENBERICHT

Inter. majus. Aktenzeichen

PCT/DE 99/02844

**A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**  
IPK 7 G06F1/00

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)  
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 752 636 A (SUN MICROSYSTEM) 8. Januar 1997 (1997-01-08) Spalte 3, Zeile 11 - Spalte 4, Zeile 19 Spalte 6, Zeile 35 - Spalte 10, Zeile 37; Ansprüche; Abbildungen 3,5	1-10
A	US 5 611 048 A (JACOBS ET AL.) 11. März 1997 (1997-03-11) Spalte 2, Zeile 1 - Zeile 33 Spalte 5, Zeile 65 - Spalte 11, Zeile 25; Anspruch 1; Abbildungen 5-8	1-10

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfindeterischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfindeterischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"a" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

16. Februar 2000

Absendedatum des internationalen Recherchenberichts

24/02/2000

Name und Postanschrift der internationalen Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3018

Bevollmächtigter Beauftragter

Soler, J

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE 99/02844

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 752636	A	08-01-1997	US	5734718 A	31-03-1998
			JP	9231174 A	05-09-1997
US 5611048	A	11-03-1997	KEINE		